ESTADO DO MARANHÃO
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

RESOL-GP - 132017
Código de validação: E96E74602C
Dispõe sobre a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Maranhão e dá outras providências.
O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a Resolução nº 211 do Conselho Nacional de Justiça, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a necessidade do uso responsável de conteúdos existentes na Internet, para uso exclusivo no desenvolvimento das atividades do Judiciário;
CONSIDERANDO a necessidade de se estabelecer controles que assegurem o uso seguro da infraestrutura de comunicação e armazenamento de dados por magistrados, servidores, agentes públicos e prestadores de serviços;
CONSIDERANDO que o Tribunal de Justiça do Maranhão gera e utiliza informações no exercício de suas competências constitucionais, legais e regulamentares e que essas informações devem permanecer íntegras, disponíveis e, quando for o caso, com sigilo resguardado;
CONSIDERANDO a importância da adoção de boas práticas relacionadas à proteção da informação, preconizadas pelas normas NBR ISO/IEC 27001:2013, NBR ISO/IEC 27002:2013, NBR ISO/IEC 27005:2011 e pelas Diretrizes para Gestão da Segurança da Informação no âmbito do Poder Judiciário;
CONSIDERANDO que a Resolução nº 62/2017 determina a necessidade de elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos em todos os níveis da instituição e em harmonia com as diretrizes nacionais preconizadas pelo Conselho Nacional de Justiça;
R E S O L V E, ad referendum:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1ºA Política de Segurança da Informação tem por objetivo controlar o acesso à infraestrutura de comunicação e armazenamento de dados, evitando que os recursos computacionais do Judiciário sejam utilizados em desrespeito às leis, às normas, aos costumes e à dignidade da pessoa humana, protegendo o ambiente computacional do Judiciário contra ameaças advindas de acessos à rede corporativa e aos ativos de informática, garantindo a integridade, a autenticidade, a confidencialidade e a disponibilidade das informações.
§1º A Política de Segurança da Informação se aplica a todos os magistrados, servidores efetivos e requisitados, ocupantes de cargo em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informática do Judiciário.
§2º O Comitê Gestor de Segurança da Informação é o responsável pela gestão da Política de Segurança da Informação, nos termos da Resolução n° 6/2017.
§3º São objetivos da Política de Segurança da Informação:
I – instituir diretrizes estratégicas, responsabilidades e competências, visando a garantia da segurança da informação;
II – promover ações necessárias à implementação, à manutenção da segurança da informação;
III – combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação, o sigilo e a imagem do Judiciário;

IV – promover a conscientização e a capacitação de recursos humanos em segurança da informação.
Art. 2º A Diretoria de Informática e Automação é a unidade responsável pela elaboração e execução da Política de Segurança da Informação no Poder Judiciário do Maranhão, competindo-lhe aplicar as políticas de segurança e contingência, garantindo os princípios de segurança da informação no Judiciário;
§1º Compete exclusivamente aos servidores lotados na Diretoria de Informática e Automação a gestão do ambiente computacional, bem como o acesso com perfil de administração aos sistemas e serviços do Judiciário.
§2º Cabe às chefias imediatas orientar e supervisionar seus subordinados, promovendo a adequada utilização dos ativos e recursos de informática, zelando pelos princípios da segurança da informação, conforme disciplinado nesta Resolução.
Art. 3º Para afeito desta Resolução entende-se:
I - ameaça: é a possibilidade de um agente, interno ou externo, explorar acidentalmente ou propositalmente uma vulnerabilidade provocando dano, perda ou prejuízo, para uma informação, um sistema, órgão ou entidade da estrutura organizacional do Judiciário;
II - Internet: sistema global de redes de computadores interligadas que utilizam um conjunto próprio de protocolos, com o propósito de servir progressivamente usuários no mundo inteiro;
III - intranet: ambiente de rede interna do Poder Judiciário do Estado do Maranhão, composta pelo conjunto de redes locais e seus ativos e recursos de informática utilizados para sua formação;
IV - prestador de serviço: toda e qualquer pessoa que possui uma relação contratual ou de convênio com o Judiciário;
V - agente público: toda e qualquer pessoa que exerce uma atribuição pública em sentido lato, seja estagiário, ocupante de função, cargo ou de emprego público;
VI - rede corporativa: sistema de transmissão de dados que transfere informações entre diversos equipamentos de uma mesma corporação;
VII - informação: é um ativo, que tem valor para organização e necessita ser adequadamente protegido. A informação existe sob as mais diversas formas, incluindo material impresso, escrito, falado, filmes, conversas ou meios analógicos, eletrônicos, óticos ou magnéticos como CDs, disquetes, discos de armazenamento em equipamentos servidores, estações de trabalho e qualquer outro meio existente ou que venha a ser criado;
VIII - ativo de informática: é todo elemento que manipula e processa a informação, inclusive a própria informação, o meio em que ela é armazenada, os equipamentos com os quais ela é manuseada, transportada e descartada. Figuram como ativos, além da informação, microcomputadores e seus acessórios, notebooks, impressoras, computadores servidores, dispositivos de armazenamento de dados, sistemas de informação, equipamentos de conexão de rede, dispositivos e equipamentos de transmissão de dados ou quaisquer outros dispositivos que venham a processar informação ou prover acesso aos recursos de informática;
IX - confidencialidade: é o princípio da segurança da informação o qual define que toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de acesso e uso apenas aos indivíduos para os quais elas são destinadas;
X - integridade: é o princípio da segurança da informação o qual define que toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais;
XI - disponibilidade: é o princípio da segurança da informação o qual define que toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para o melhor desempenho de suas atribuições e/ou funções;
XII - usuário: é considerado todo indivíduo, incluindo magistrados, servidores, prestadores de serviços, ou qualquer outra pessoa, devidamente credenciado para acesso aos ativos de informática do Poder Judiciário;
XIII - login: é parte da credencial do usuário com prévio cadastramento através de sua matrícula ou identificador único, no sistema, software ou serviço, de modo a garantir a individualização do seu proprietário;
XIV - senha: é parte da credencial do usuário, formada por um conjunto de caracteres alfabéticos,

numéricos ou alfanuméricos, de caráter pessoal, confidencial e intransferível, para uso nos sistemas, softwares e serviços de informática;
XVI - credencial: é a combinação do login e senha, utilizada, ou não, em conjunto com outro mecanismo de autenticação, que visa legitimar e conferir autenticidade ao usuário na utilização da infraestrutura e recursos de informática;
XVI – software malicioso: é o termo coletivo para descrever programas com intenções maliciosas, incluindo vírus, worms, trojans ou qualquer outra praga digital que ponham em risco a confidencialidade, integridade e disponibilidade das informações.
XVII - spam: é o termo usado para referir-se a mensagens não solicitadas, enviadas a um grande número de indivíduos e com conteúdo geralmente comercial, fraudulento ou impróprio;
XVIII - software: é qualquer programa ou conjunto de programas de computador;
XIX - rede local: é considerada como o ambiente de rede interna de cada edificação do Poder Judiciário do Estado do Maranhão, composta por seus ativos e recursos de informática, assim como seus meios físicos e lógicos de conexão;
XX - rede corporativa de dados do Poder Judiciário: é considerada como o ambiente computacional disponibilizado, gerenciado e mantido pelo Poder Judiciário do Estado do Maranhão, composta pelo conjunto de redes locais, intranet, extranet, softwares, sistemas de informação, áreas de armazenamento de dados, bases de dados e os ativos e recursos de informática utilizados para sua formação;
XXI - correio eletrônico ou e-mail: é o serviço de comunicação de mensagens eletrônicas entre usuários, composto por programas de computador e equipamentos centrais de processamento, responsáveis pelo envio e recebimento das mensagens, bem como pela administração das caixas postais;
XXII - área de armazenamento de dados: trata de espaço reservado, limitado, acessível através de rede de computadores, onde os usuários podem guardar suas informações digitais, preferencialmente documentos de trabalho;
XXIII - download: é o termo usado para recebimento de arquivos através de uma rede de computadores que utiliza os padrões TCP/IP, de um computador remoto para um computador local;
XXIII - upload: é o termo usado para envio de arquivos através de rede de computadores que utiliza os padrões TCP/IP, de um computador local para um computador remoto (ação inversa do download).

CAPÍTULO II
DOS USUÁRIOS

Art. 4ºOs usuários do Poder Judiciário deverão utilizar os ativos de informática para desenvolvimento de atividades exclusivamente jurisdicionais ou administrativas, fazendo uso de suas credenciais de acesso, exclusivamente.
Parágrafo único. As credenciais de acesso são pessoais e intransferíveis; toda e qualquer ação executada pelo usuário utilizando uma determinada credencial será de responsabilidade exclusiva do mesmo, devendo este zelar por sua confidencialidade.
Art. 5º O credenciamento de usuários será realizado pela Diretoria de Informática e Automação, após solicitação efetuada pela chefia imediata do usuário, através dos meios de comunicação oficial utilizada pelo Judiciário.
§1º Os direitos e permissões de acesso requeridos pela chefia imediata do usuário objetivarão atender exclusivamente à necessidade do serviço e serão avaliados pela Diretoria de Informática e Automação, que habilitará o acesso exclusivamente aos recursos e sistemas necessários à execução das atividades do setor requisitante e observando sempre o disposto nesta Resolução.
§2º Mudança de lotação, atribuições, afastamento definitivo ou temporário do usuário deverão ser automaticamente comunicados à Diretoria de Informática e Automação pela Diretoria de Recursos Humanos, para procedimentos de ajuste ou cancelamento de credenciais de acesso.
§3º Nos casos de afastamento definitivo ou temporário de usuário não pertencente ao quadro de servidores do Judiciário caberá à sua chefia imediata a solicitação de cancelamento ou bloqueio, através dos meios de comunicação oficiais utilizados pelo TJMA, cabendo a essa chefia o ônus por qualquer uso indevido da credencial do usuário, decorrente da não comunicação de seu afastamento.
Art. 6º Aos usuários compete:

I – zelar pelos princípios de segurança da informação, principalmente no que concerne à confidencialidade e integridade das credenciais de acesso;
II – zelar pela segurança das informações, seguindo os princípios de confidencialidade, integridade e disponibilidade, manuseando corretamente os programas de computador, ligando e desligando adequadamente os equipamentos, fechando ou bloqueando os programas ou sistemas quando não estiverem utilizando, não deixando informações importantes desprotegidas, independentemente de sua forma;
III - não compartilhar, não divulgar e certificar-se de não ser observado ao digitar sua senha;
IV - alterar as senhas sempre que julgar necessário, não usar a mesma senha para todos os serviços;
V - utilizar senhas fortes. Uma senha forte, é aquela que é difícil de ser descoberta e fácil de ser lembrada;
VI – comunicar imediatamente à Diretoria de Informática e Automação qualquer suspeita de atos indevidos, extravio de credencial, acesso não autorizado, comprometimento de informação por software malicioso ou qualquer outra suspeita de ação que possa ser lesiva à Administração;
VII – zelar pela segurança dos ativos de informática, certificando-se da inexistência de software malicioso em pendrives, CD's ou dispositivos afins antes da sua utilização.
Art. 7º É considerado descumprimento da política de segurança da informação, ficando sujeito a penalidades:
I – fornecer, por qualquer motivo, sua credencial de acesso para outrem;
II – fazer uso da credencial de outrem para acesso e utilização de ativos ou recursos de informática, como sistemas, Internet, intranet e correio eletrônico;
III - obter acesso não autorizado a qualquer outro computador, rede, banco de dados ou informações guardadas eletronicamente;
IV – omitir informação à Diretoria de Informática e Automação, no que concerne ao disposto nos §§ 2º e 3º do Art. 3º;
V - utilizar os ativos de informática para armazenamento, distribuição, divulgação ou manipulação de conteúdos diversos do trabalho que exerça, com teor comercial, sexual, ofensivo, difamatório, discriminatório e agressivo à dignidade humana;
VI - utilizar os ativos de informática de forma a interferir no trabalho dos demais servidores/usuários ou que comprometa o desempenho e/ou a segurança das informações existentes na rede corporativa de dados do Poder Judiciário;
VII - instalar e/ou configurar ativos de informática sem o acompanhamento e a homologação da Diretoria de Informática e Automação;
VIII - fazer uso de qualquer tipo de ativo de informática não contratado, licenciado ou homologado pela Diretoria de Informática e Automação;
IX - instalar e/ou configurar acesso externo à rede corporativa do Judiciário.
Parágrafo único. Além das hipóteses anteriormente previstas, incorre em descumprimento da política de segurança da informação qualquer outra prática não autorizada expressamente pela Diretoria de Informática e Automação que importe em dano aos ativos de informática existentes na rede corporativa de dados do Poder Judiciário.

CAPÍTULO III
DO ACESSO À INTERNET

Art. 8º O acesso à Internet será disponibilizado para magistrados, servidores, prestadores de serviço e agentes públicos, observando a necessidade de uso responsável de conteúdos existentes na Internet, exclusivamente para o desenvolvimento das atividades do Judiciário.
§1º No período das 00h00 as 07h59min o acesso será liberado a todos os sítios, excluindo-se aqueles que possuam natureza imprópria ou ilegal.
§2º No período das 08h00 as 18h00 o acesso será restrito apenas aos sítios de:
I – Órgãos do Judiciário, Executivo, Legislativo e Ministério Público;
II – Empresas Públicas e de Economia Mista;
III – Bancos e instituições financeiras;
IV – Pesquisa de jurisprudência;
V – Associações de classe e sindicatos;
VI – Correio eletrônico;

VII – Sítios de interesse do Judiciário.
§3º No período das 18h01min às 23h59min o acesso será liberado a todos os sítios, excluindo-se aqueles que possuam natureza imprópria ou ilegal.
§4º Nos fins de semana o acesso será liberado a todos os sítios, excluindo-se aqueles que possuam natureza imprópria ou ilegal.
§5º O Comitê Gestor de Segurança da Informação poderá autorizar, após parecer técnico da Diretoria de Informática e Automação, a criação de grupos de usuários com permissões especiais de acesso.
Art. 9º O acesso à Internet, realizado por meio de ativos de tecnologia de informação e comunicações do Judiciário, deve ser autorizado, identificado e registrado.
§1º Os registros de acessos aos sítios da Internet devem ser preservados em conformidade com a legislação em vigor.
§2º Compete a Diretoria de Informática elaborar e implementar mecanismos de auditoria e conformidade, com o objetivo de garantir a exatidão dos registros de acesso e avaliar sua conformidade com as normas em vigor.
Art. 10. Cabe a Diretoria de Informática e Automação propor e implementar a política de controle de acesso à Internet no Judiciário, competindo-lhe:
I – aplicar políticas de restrição de acesso a sites;
II – aplicar regras que limitem a velocidade de meios de comunicação;
IV – realizar perícias, auditorias e monitoramento de serviços históricos de acesso a sites pelos usuários e conteúdo de mensagens e e-mails;
V – aplicar controles necessários para monitorar, identificar, filtrar e bloquear acesso às informações consideradas inadequadas ou não relacionadas às atividades jurisdicionais ou administrativas, especialmente sites de entretenimento, conteúdo agressivo, drogas, pornografia, pedofilia, jogos, redes sociais, bate-papos, sites com conteúdo que incentivem pirataria, bem como restringir o acesso a serviços que podem tornar vulneráveis os ativos de informática às invasões externas e ataques, em suas mais diferentes formas, levando a perda de princípios de Segurança da Informação.
§1º Na constatação da existência de acessos aos sites relacionados no inciso V deste artigo, deverá a Diretoria de Informática e Automação comunicar o fato à Administração para as providências cabíveis.
§2º Caso seja detectado algum controle que restrinja o acesso ao conteúdo relacionado às atividades jurisdicionais ou administrativas, o usuário deverá comunicar à Diretoria de Informática e Automação, para providências cabíveis.
§3º É facultado à Diretoria de Informática e Automação a aplicabilidade sumária dos incisos deste artigo, sem o consentimento ou aviso prévio dos indivíduos envolvidos ou interessados.
Art. 11. É considerado uso indevido da Internet, sujeito às penalidades:
I – acessos aos sites não relacionados às atividades jurisdicionais ou administrativas;
II – download e upload de arquivos alheios às atividades jurisdicionais ou administrativas.

CAPÍTULO IV
DO USO DA REDE LOCAL, DA INTRANET E DA REDE SEM FIO

Art. 12. O acesso à rede local, à intranet e à rede sem fio será realizado mediante identificação com credencial única de acesso, observando sempre o disposto nesta Resolução.
Parágrafo único. O acesso externo à rede corporativa, quando essencial ao desenvolvimento das atividades do Judiciário, dar-se-á mediante Rede Privada Virtual – VPN, cabendo à Diretoria de Informática e Automação analisar, aprovar e implementar a solução.
Art. 13. Compete à Diretoria de Informática e Automação:
I – garantir os Princípios de Segurança da Informação aos recursos e ativos de rede local, intranet e rede sem fio;
II – disponibilizar aos usuários áreas de armazenamento de informações na rede de computadores;
III – disciplinar, limitar, auditar e periciar arquivos e informações guardadas nas áreas de armazenamento disponíveis.
Art. 14. É considerado uso indevido da rede local, da intranet e da rede sem fio, sujeito às penalidades:
I – manter armazenados nos ativos da rede local, arquivos e informações que não estejam relacionados às atividades jurisdicionais ou administrativas, incluindo arquivos de software,

documentos, imagens, áudio e vídeo;
II – utilizar os recursos e ativos de informática para transferência de arquivos que não estejam relacionados às atividades jurisdicionais ou administrativas.
Art. 15. Compete ao usuário garantir a confidencialidade, integridade e disponibilidade das informações armazenadas fora dos recursos da rede local, em disco rígido dos computadores, notebooks, pendrives ou outros dispositivos de armazenamento de dados.

CAPÍTULO V
DO USO DO CORREIO ELETRÔNICO

Art. 16. Cada usuário, de acordo com a necessidade do serviço, terá acesso a uma caixa postal de correio eletrônico identificada unicamente pela sua credencial, de uso pessoal e intransferível.
§1º As caixas postais disponibilizadas para usuários somente poderão ser utilizadas para transmitir e receber informações relacionadas às atividades jurisdicionais ou administrativas.
§2º Fica determinado que, caso não sejam detectados acessos regulares às caixas postais dos usuários, em um prazo superior a 60 (sessenta) dias, ficará a caixa postal respectiva desativada por motivos de segurança.
Art. 17. As unidades administrativas e judiciais terão uma ou mais caixas postais de correio eletrônico, de acordo com as necessidades de seus organogramas, que deverão ser acessadas regularmente por usuários daquela unidade, devidamente autorizados pela chefia imediata.
§1º As caixas postais das unidades deverão ser utilizadas preferencialmente para as comunicações oficiais entre as unidades.
§2º Os endereços de correio eletrônico das unidades poderão ser divulgados através da intranet e Internet, de acordo com a conveniência dessas.
§3º No caso de afastamento temporário ou provisório dos usuários autorizados a manipular as caixas postais das unidades caberá a chefia imediata garantir, através de requerimento à Diretoria de Informática e Automação, que o usuário substituto mantenha o acesso regular às caixas postais, zelando e garantindo pelos princípios de segurança da informação.
§4º Fica determinado que, caso não sejam detectados acessos regulares às caixas postais das unidades administrativas e suas subdivisões, em um prazo superior a 60 (sessenta) dias, ficará a caixa postal respectiva desativada por motivos de segurança.
Art. 18. Compete à Diretoria de Informática e Automação:
I – criar, alterar ou excluir caixas postais de usuários e unidades de trabalho;
II – impor controles e limites à utilização dos serviços de correio eletrônico, observando sempre o disposto nesta Resolução;
III – aplicar políticas de limites de área de armazenamento necessária para mensagens, ficando o usuário impedido de receber novas mensagens quando ultrapassar estes limites;
IV – aplicar políticas que limitem o tamanho máximo de mensagens enviadas ou recebidas, incluindo arquivos anexados, bloqueando mensagens que ultrapassem os limites estabelecidos;
V– aplicar controles de verificação de anexos enviados e recebidos, ficando vedada a troca de arquivos não vinculados às atividades jurisdicionais ou administrativas;
VI – aplicar controles de verificação quanto à presença de conteúdo indevido, impróprio ou malicioso, bloqueando as mensagens, facultado à Diretoria de Informática e Automação o aviso automático ao remetente ou destinatário;
VII – revisar, em caso de necessidade e observando sempre o disposto nesta Resolução, os limites e controles estabelecidos, quando solicitado pela chefia imediata do usuário, com a devida justificativa.
Art. 19. É considerado uso indevido do serviço de correio eletrônico, sujeito às penalidades:
I – tentativa de acesso ou acesso não-autorizado às caixas postais de terceiros;
II – envio de informações confidenciais, classificadas, privilegiadas ou proprietárias, inclusive senhas e dados, para indivíduos ou organizações não autorizadas;
III – envio de conteúdo obsceno, ilegal, não-ético, comercial, pessoal, mensagens do tipo corrente, entretenimento, SPAM, propaganda política, boatos e mensagens enganosas;
IV – envio de mensagens ofensivas que causem molestamento ou tormento ou denigram a imagem da instituição;
V – envio de mensagens contendo softwares maliciosos ou quaisquer formas de rotinas de programação prejudiciais ou danosas às estações de trabalho ou ao sistema de correio;

VI – outras atividades que possam afetar, de forma negativa, o Poder Judiciário, seus magistrados e servidores, fornecedores ou parceiros.

§1º O uso do correio eletrônico para veiculação de campanhas internas de caráter social ou informativo de grande relevância deverá ser incentivado mediante aprovação pela Administração e observando sempre o disposto nesta Resolução.

§2º Os usuários que receberem mensagens indesejáveis, como as elencadas nos incisos deste artigo, devem encaminhá-las à Diretoria de Informática e Automação, no endereço eletrônico informatica@tjma.jus.br, para que sejam tomadas as devidas providências.

CAPÍTULO VI
DO ACESSO AOS SISTEMAS DE INFORMAÇÃO

Art. 20. Cada usuário, de acordo com a necessidade do serviço, terá acesso aos sistemas de informação do Judiciário, identificado unicamente pela sua credencial, de uso pessoal e intransferível.

§1º O acesso aos sistemas será disponibilizado aos usuários somente para execução das atividades jurisdicionais ou administrativas.

§2º No caso de sistemas acessados mediante uso de certificação digital, a mesma será fornecida aos usuários, observando-se as regras da Resolução nº 27/2013TJ.

§3º As credenciais de acesso aos sistemas são pessoais e intransferíveis; toda e qualquer ação executada pelo usuário utilizando uma determinada credencial será de responsabilidade exclusiva do mesmo, devendo este zelar por sua confidencialidade.

§4º A habilitação de usuários para uso dos sistemas será realizada pela Diretoria de Informática e Automação, após solicitação efetuada pela chefia imediata do usuário, através dos meios de comunicação oficial utilizada por este órgão.

Art. 21. É considerado uso indevido dos sistemas de informação, ficando sujeito a penalidades:

I - fornecer, por qualquer motivo, sua credencial de acesso a sistema de informação para outrem;

II - fazer uso da credencial de outrem para acesso e utilização de sistema de informação;

III - utilizar sistema de informação de forma a interferir no trabalho dos demais usuários ou que comprometa o desempenho e/ou a segurança das informações do Poder Judiciário;

IV - divulgar informações sigilosas ou reservadas, 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, com o fim de obter vantagem indevida para si ou para outrem ou para causar dano.

Parágrafo único. Além das hipóteses anteriormente previstas, incorre em descumprimento da política de segurança da informação qualquer outra prática não autorizada expressamente pela Diretoria de Informática e Automação que importe em dano aos sistemas de informação existentes no Poder Judiciário.

CAPÍTULO VII
DAS PENALIDADES

Art. 22. O usuário identificado como infrator de alguma das disposições desta Resolução poderá ter sua credencial bloqueada, considerado o interesse da Administração, a partir da solicitação para instauração de processo administrativo disciplinar, podendo o bloqueio perdurar durante o trâmite da sindicância ou inquérito administrativo, sempre dando ciência à chefia imediata para reorganização das tarefas.

Art. 23. O descumprimento das disposições contidas nesta Resolução poderá caracterizar infração funcional, a ser apurada em processo administrativo disciplinar.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 24. Deverá se elaborado pela Diretoria de Informática e Automação um Plano de Continuidade de Negócios que estabeleça estrutura mínima de recursos para o desenvolvimento da resiliência organizacional, capaz de garantir o fluxo das informações críticas e salvaguardar o interesse das partes, a reputação e imagem do Judiciário.

Art. 25. A utilização dos recursos e ativos de informática do Poder Judiciário, incluindo a Internet e intranet deverá ser monitorada e auditada através das credenciais do usuário.

Art. 26. O conteúdo desta Resolução estará disponível para consulta pelos usuários através da intranet do Poder Judiciário.
Art. 27. Os casos omissos serão resolvidos pela Presidência do Tribunal de Justiça.
Art. 28. Esta Resolução entrará em vigor na data de sua publicação, revogada a Resolução 56/2008.
TRIBUNAL DE JUSTIÇA DO ESTADO DO MARANHÃO, Palácio da Justiça "Clóvis Bevilácqua", em São Luís.

Desembargador CLEONES CARVALHO CUNHA
PRESIDENTE

Documento assinado. SÃO LUÍS - TRIBUNAL DE JUSTIÇA, 23/03/2017 12:52 (CLEONES CARVALHO CUNHA)

Informações de Publicação

Edição	Disponibilização	Publicação
5/2018	12/01/2018 às 10:50	15/01/2018

Imprimir