PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

RESOLUÇÃO Nº 222, DE 3 DE FEVEREIRO DE 2016.

Institui a Política de Segurança da Informação e Comunicação da Justiça Militar da União e dá outras providências.

O SUPERIOR TRIBUNAL MILITAR, no uso de suas atribuições legais e regimentais, e tendo em vista a decisão do Plenário na 1ª Sessão Administrativa, realizada em 3 de fevereiro de 2016, ao apreciar o Expediente Administrativo nº 6/2016,

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações, regulamentada pelo Decreto nº 7.724, de 16 de maio de 2012;

CONSIDERANDO o Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

CONSIDERANDO a Resolução nº 90, de 29 de setembro de 2009, do Conselho Nacional de Justiça, que dispõe sobre os requisitos de nivelamento de tecnologia da informação no âmbito do Poder Judiciário, alterada pela Resolução nº 136, de 13 de julho de 2011, do Conselho Nacional de Justiça;

CONSIDERANDO a Resolução nº 194, de 28 de agosto de 2013, do Superior Tribunal Militar, que dispõe sobre a criação do Comitê Gestor de Segurança da Informação e define suas competências no âmbito da Justiça Militar da União;

CONSIDERANDO a Resolução nº 215, de 16 de dezembro de 2015, do Conselho Nacional de Justiça, que dispõe, no âmbito do Poder Judiciário, sobre o acesso à informação e a aplicação da Lei nº 12.527, de 18 de novembro de 2011;

CONSIDERANDO as recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de práticas confiáveis para a gestão da Segurança da Informação;

CONSIDERANDO a gestão de riscos identificados no Plano de Segurança Orgânica (PSO) das unidades da Justiça Militar da União;

CONSIDERANDO a necessidade de estabelecer e orientar a condução das diretrizes de salvaguarda das informações e dos serviços de transmissão de dados na Justiça Militar da União,

RESOLVE:

Art. 1º Fica instituída a Política de Segurança da Informação e Comunicação (PSIC) como mecanismo preventivo de proteção de dados e de sua transmissão, equipamentos, processos e documentos produzidos e custodiados no âmbito da Justiça Militar da União (JMU), sendo aplicável à informação em qualquer meio ou suporte, seja este papel, nato-digital ou digitalizado e os serviços de telemática, que incluem as redes digitais, sistemas de videoconferências e de transmissão e gravação de seções de audiência.

§ 1º Os usuários internos e externos de informações e comunicações produzidas ou custodiadas pela JMU estão sujeitos às disposições estabelecidas na PSIC;

§ 2º As ações da PSIC serão implementadas e acompanhadas pelas unidades da Justiça Militar da União;

§ 3º São consideradas unidades da JMU:

a) as unidades que integram a estrutura orgânica do Superior Tribunal Militar (STM), conforme estabelece a Resolução nº 217, de 9 de setembro de 2015;

b) a Auditoria de Correição;

c) as Auditorias das Circunscrições Judiciárias Militares.

SEÇÃO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 2º Para os efeitos desta Resolução, consideram-se:

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

II - dados processados: dados submetidos a qualquer operação ou tratamento por meio de processamento eletrônico ou por meio automatizado com o emprego de tecnologia da informação;

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

IV - informação sigilosa: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais de sigilo;

V - informação pessoal: informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem;

VI - 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;

VII - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;

VIII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;

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

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

XI - informação atualizada: informação que reúne os dados mais recentes sobre o tema, de acordo com sua natureza, com os prazos previstos em normas específicas ou conforme a periodicidade estabelecida nos sistemas informatizados que a organizam;

XII - documento preparatório: documento formal utilizado como fundamento da tomada de decisão ou de ato administrativo, a exemplo de pareceres e notas técnicas;

XIII - confidencialidade: garantia de que a informação seja acessada somente pelas pessoas que tenham autorização para tal;

XIV - custodiante: servidor ou unidade que detenha a posse, mesmo que transitória, de informação produzida ou recebida pela JMU;

XV - gestor da informação: servidor, unidade ou estrutura *ad hoc* que, no exercício de suas competências, seja responsável pela produção de informações, pela definição de requisitos de soluções de tecnologia da informação ou pelo tratamento, ainda que temporário, de informações de propriedade de pessoa física ou jurídica entregues à JMU;

XVI - incidente em segurança da informação: fraude, sabotagem, desvio, falha de equipamentos, acessos não autorizados, mau uso, extravio, furto ou evento indesejado ou inesperado que possa comprometer as atividades da JMU ou ameaçar a segurança da informação e comunicação;

XVII - segurança da informação: proteção da informação contra ameaças para garantir a continuidade das atividades da JMU e minimizar os riscos;

XVIII - usuário externo: qualquer pessoa física ou jurídica que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pela JMU e que não seja caracterizada como usuário interno;

XIX - usuário interno: qualquer servidor, prestador de serviço, estagiário ou qualquer outro colaborador que tenha acesso, de forma autorizada, a informações produzidas ou custodiadas pela JMU;

XX - colaborador: os estagiários e as pessoas contratadas como prestadoras de serviço habitual (continuado) nas unidades da JMU;

XXI - parceiro: as pessoas que venham a prestar serviços eventuais nas unidades da JMU;

XXII - acessibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos arquivos correspondentes sempre que necessitarem, respeitando-se a legislação em vigor;

XXIII - flexibilidade: garantia de que os sistemas de telemática tenham capacidade de manter as conexões de rede e *links*, por meios alternativos de enlaces, de forma a assegurar, permanentemente, comunicações eficientes, confiáveis e seguras;

XXIV - integração: garantia de que os sistemas tenham capacidade de comunicar-se uns com os outros, serem mutuamente acessíveis, quando houver a necessidade técnica ou funcional para tal.

SEÇÃO II
DAS FINALIDADES

Art. 3º A Política de Segurança da Informação (PSIC) da JMU tem como objetivo prevenir a ocorrência de vulnerabilidades na gestão documental e da tecnologia da informação e comunicação, no âmbito desta Justiça Especializada.

Art. 4º A Segurança da Informação e Comunicação (SIC) na Justiça Militar da União abrange aspectos físicos, tecnológicos e humanos e orienta-se pelos princípios da confidencialidade, disponibilidade e integridade.

Art. 5º A SIC é baseada em três fundamentos:

I - segurança física: baliza a definição das políticas e procedimentos que tratam dos controles de acesso e circulação de pessoas e de veículos, bem como do acesso a equipamentos, processos e documentos em suporte papel, nato-digitais ou digitalizados;

II - segurança dos recursos humanos: norteia os procedimentos a serem criados para conscientização de todos os participantes do processo de implantação da PSIC, a fim de que tal processo ocorra de forma natural e efetiva;

III - segurança lógica: orienta o estabelecimento de normas e procedimentos visando auxiliar os participantes na utilização de todos os recursos tecnológicos para tramitação dos Processos Eletrônicos, no acesso à internet e à intranet, nas estações de trabalho, na utilização de correio eletrônico, de videoconferências, de impressoras, de equipamentos móveis de propriedade da JMU, como *tablets* e *smartphones*, de *backups* e de prevenção e proteção contra vírus e *malware*.

SEÇÃO III
DO USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

Art. 6º Os recursos de tecnologia da informação disponibilizados nas unidades da Justiça Militar da União destinam-se, exclusivamente, ao atendimento das necessidades do serviço.

§ 1º É proibida a utilização dos recursos de tecnologia da informação disponibilizados pela Justiça Militar da União para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais, ou que infrinja a legislação vigente.

§ 2º É vedada a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela JMU.

Art. 7º Compete à Diretoria de Tecnologia da Informação (DITIN) prover e controlar o uso dos recursos de tecnologia da informação, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional.

Art. 8º Aos usuários são fornecidos mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, vedada sua divulgação a terceiros.

§ 1º Pelo uso indevido dos mecanismos de identificação respondem quem permitiu ou facilitou o acesso e quem os utilizou.

§ 2º O acesso aos recursos de tecnologia da informação é concedido mediante solicitação de titular de unidade da JMU à DITIN.

§ 3º Todas as operações realizadas com uso dos recursos de tecnologia da informação serão registradas para fins de auditoria.

§ 4º A Diretoria de Pessoal (DIPES) deve comunicar imediatamente à DITIN as movimentações, afastamentos e desligamento de servidores e estagiários da JMU para fins de alteração nas permissões de acesso aos recursos de tecnologia.

§ 5º Os titulares das unidades da JMU devem pessoalmente realizar, quando possível, ou solicitar imediatamente à DITIN a alteração nas permissões de acesso aos recursos de tecnologia dos servidores, estagiários e prestadores de serviço sob sua responsabilidade, sempre que houver necessidade e quando ocorrer violação do disposto nesta Resolução.

§ 6º A DITIN realizará as alterações nas permissões de acesso no mesmo dia do recebimento da demanda, ou até o expediente seguinte no caso de chamados abertos após as 16 horas, dando imediata ciência ao demandante quanto à efetivação do procedimento.

SEÇÃO IV
DAS MEDIDAS DE CONTROLE

Art. 9º A Política de Segurança da Informação (PSIC) da JMU não é limitada à segurança da Tecnologia da Informação e Comunicação (TIC), dela fazendo parte um conjunto de diretrizes, normas e procedimentos específicos de segurança destinados a reger o funcionamento seguro das atividades de gestão documental, de TI e de Telemática dentro da Instituição, englobando regras para pessoas, processos e tecnologias, e observando os seguintes princípios: confidencialidade, integridade, acessibilidade, disponibilidade, autenticidade, flexibilidade e integração.

Art. 10. A Segurança da Informação e Comunicação (SIC) é regida pelas seguintes regras:

I - simplicidade: fácil leitura, compreensão e aplicação, definindo o papel de cada integrante da JMU;

II - legalidade: conformidade com a legislação vigente, garantindo níveis de privacidade aos usuários;

III - objetividade: elaboração de normas pontuais específicas e concisas;

IV - estratégia: estabelecimento de metas específicas de segurança;

V - responsabilidade: definição dos responsáveis pela informação e pela correta utilização e divulgação;

VI - normatividade: definição das penalidades cabíveis em casos de violação e de não cumprimento das regras definidas.

SEÇÃO V
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 11. Compete ao gestor da informação:

I - adotar critérios de classificação e procedimentos de acesso às informações, observados os dispositivos legais e normas internas referentes ao sigilo e a outros requisitos de classificação;

II - propor regras específicas para o uso das informações.

Art. 12. Compete ao custodiante da informação:

I - zelar pela segurança da informação sob sua custódia, conforme os critérios definidos pelo respectivo gestor da informação;

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

III - comunicar ao gestor eventuais limitações ao cumprimento dos critérios definidos para segurança da informação.

Art. 13. Compete às unidades da JMU:

I - garantir a segurança da informação e comunicação em seu âmbito, cumprindo e fazendo cumprir as normas estabelecidas na Política de Segurança da Informação e Comunicação (PSIC) da JMU e demais diretivas relacionadas ao emprego dos sistemas e equipamentos de TIC;

II - implementar e acompanhar ações da PSIC;

III - colaborar na conscientização dos usuários internos em relação aos conceitos e às práticas de Segurança da Informação e Comunicação (SIC);

IV - incorporar aos processos de trabalho práticas inerentes à SIC;

V - adotar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de violação à PSIC por parte dos usuários internos.

Art. 14. Compete à Escola Nacional de Formação e Aperfeiçoamento da Justiça Militar da União (ENAJUM) participar, juntamente com a DIPES e em coordenação com a Auditoria de Correição, na elaboração de normas de segurança pela DITIN, para o emprego de videoconferência em atividades de capacitação, observado o previsto no inciso XIII do art. 22 desta Resolução.

Art. 15. Compete à Auditoria de Correição propor, em colaboração com a DITIN, as normas para o emprego da videoconferência na 1ª instância e suas atualizações, observado o previsto no inciso XIII do art. 22 desta Resolução.

Art. 16. Compete às Auditorias e Foros:

I - exigir e controlar, em colaboração com a DITIN, a assinatura do Termo de Compromisso e Responsabilidade (TCR) por parte dos usuários internos e parceiros de sua unidade;

II - implementar os controles e monitoramentos de segurança pertinentes, sob a orientação técnica das unidades custodiantes (SESEG, DITIN e DIDOC).

Art. 17. Compete à Diretoria de Pessoal:

I - colaborar com a DITIN, conforme necessário, para a implementação de um procedimento sistematizado de controle de assinaturas de TCR, conforme previsto no § 1º do art. 19 e no inciso V do art. 22 desta Resolução;

II - participar, juntamente com a ENAJUM e em coordenação com a Auditoria de Correição, na elaboração das normas de segurança pela DITIN, para o emprego da videoconferência em atividades de capacitação, observado o previsto no inciso XIII do art. 22 desta Resolução.

Art. 18. São responsabilidades dos gestores de pessoas e de processos:

I - assegurar a implantação das normas, dos processos e dos sistemas decorrentes desta Política de Segurança da Informação e Comunicação (PSIC), bem como dos termos, atos e normas já estabelecidos pelas unidades da JMU;

II - ter postura exemplar em relação à Segurança da Informação e Comunicação (SIC), servindo como modelo de conduta para os servidores e colaboradores sob a sua gestão;

III - atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta PSIC;

IV - exigir dos servidores de seu setor e colaboradores, mesmo os parceiros eventuais, a assinatura do Termo de Compromisso e Responsabilidade (TCR), como previsto no § 1º do art. 19;

V - assessorar o Comitê Gestor da Segurança da Informação no controle e no cumprimento das normas estabelecidas e, ainda, propor a adoção de medidas preventivas ou corretivas para o aperfeiçoamento da SIC.

Art. 19. É obrigação de cada magistrado, servidor efetivo ou temporário, servidor ou militar à disposição, estagiários e prestadores de serviço continuado:

I - manter-se atualizado em relação a esta Política de Segurança da Informação e Comunicação (PSIC), seguindo rigorosamente os procedimentos e normas de Segurança da Informação e Comunicação (SIC), fiscalizando e orientando os servidores, colaboradores e parceiros sob a sua gestão;

II - buscar orientação junto aos respectivos gestores de suas unidades, quanto às normas de SIC, que, nos casos de persistência de dúvidas, devem ser esclarecidas junto à Secretaria de Segurança Institucional (SESEG), à Gerência de Sistemas da Diretoria de Tecnologia da Informação (DITIN) ou à Diretoria de Documentação e Gestão do Conhecimento (DIDOC), observando as atribuições dessas unidades como definidas nos artigos 21, 22 e 23, respectivamente;

III - comunicar aos custodiantes da informação, por meio do gestor de sua unidade, observadas as atribuições definidas nos arts. 21, 22 e 23, os casos de suspeita de comprometimento da SIC ou aqueles em que não haja absoluta segurança quanto à proteção de equipamentos e mídias, produção, divulgação, transmissão, arquivos ou outro procedimento necessário ao trato da informação.

§ 1º Todos os usuários internos, colaboradores e parceiros, para se utilizarem dos meios de Tecnologia da Informação e Comunicação (TIC) e obtenção de contas na rede, deverão assinar o Termo de Compromisso e Responsabilidade (TCR), assumindo o dever de seguir as normas estabelecidas na PSIC/JMU e nas demais regulamentações que regem o emprego desses recursos na JMU, bem como se

comprometendo a manter sigilo e confidencialidade sobre todos os ativos de informações, mesmo após afastamento ou quando desligado de qualquer órgão ou unidade da JMU.

§ 2º Os usuários internos devem zelar pela segurança das informações a que tenham acesso e comunicar ao Comitê Gestor de Segurança da Informação os incidentes de que tenham conhecimento.

SEÇÃO VI
DOS CUSTODIANTES DA INFORMAÇÃO

Art. 20. São considerados "custodiantes" da informação, para os efeitos desta Resolução, a Secretaria de Segurança Institucional (SESEG), a Diretoria de Tecnologia da Informação (DITIN) e a Diretoria de Documentação e Gestão do Conhecimento (DIDOC).

Art. 21. Compete à Secretaria de Segurança Institucional (SESEG):

I - propor as medidas e processos específicos para a Segurança da Informação e Comunicação (SIC) com base na avaliação de risco apresentada nos Planos de Segurança das unidades da JMU;

II - propor, fazer cumprir e monitorar as medidas de controle de acesso, movimentação de pessoas, veículos, materiais e equipamentos, empregando os meios eletrônicos e humanos disponíveis;

III - promover a conscientização dos colaboradores em relação à relevância da segurança para a preservação dos ativos da JMU, mediante campanhas, palestras, treinamentos e outros meios de comunicação;

IV - propor e promover a atualização das Normas de Segurança da Informação e Comunicação aprovadas pelo Comitê Gestor de Segurança da Informação (CGSI) de forma alinhada às diretrizes da JMU;

V - apresentar ao CGSI os assuntos e os temas que afetam ou tenham potencial para afetar a JMU, destacando aqueles que exijam intervenção do próprio Comitê ou de outros membros da Administração da JMU;

VI - propor modernização e atualização dos meios eletrônicos disponíveis, para o devido controle do cumprimento das normas de segurança.

Art. 22. Compete à Diretoria de Tecnologia da Informação (DITIN):

I - configurar os equipamentos, fixos e móveis, ferramentas e sistemas distribuídos ou adquiridos nas unidades da JMU e os sistemas de telemática, com todos os *softwares* de controle necessários aos requisitos de segurança estabelecidos por esta PSIC e pelas Normas de Segurança já estabelecidas na JMU;

II - segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada usuário dos sistemas, com vistas a impedir que pessoas possam excluir os registros e trilhas de auditoria das suas próprias ações;

III - garantir segurança especial para sistemas com acesso público, incluindo, quando for o caso, o ambiente educacional e de videoconferência, fazendo a guarda de evidências que permitam a rastreabilidade para fins de auditoria e investigação;

IV - atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como

pessoa física, que, para obtê-la, deverá assinar o Termo de Compromisso e Responsabilidade (TCR);

V - exigir a assinatura do TCR e o seu controle, com a colaboração das demais unidades da JMU;

VI - planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida no Sistema Eletrônico de Informações (SEI), no Processo Judicial Eletrônico (PJe), nos sistemas de telemática, incluindo aqueles de videoconferências, de gravações e transmissões de sessões plenárias e de audiências e sistemas digitais das demais áreas da administração da JMU;

VII - administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a JMU;

VIII - implantar comandos que gerem registros auditáveis para retirada e transporte de mídias das informações enquadradas nas medidas de controle para pessoas, processos e tecnologias, regidos pelos princípios da confidencialidade, integridade, acessibilidade, disponibilidade e autenticidade, nos ambientes abrangidos pela Política de Segurança da Informação e Comunicação (PSIC) da JMU;

IX - gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes, bem como para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências;

X - realizar auditorias periódicas de configurações técnicas e análise de riscos, para proteção das informações da JMU contra código malicioso, e garantir que todas as novas informações só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejado;

XI - monitorar o ambiente de TI, gerando indicadores e históricos de: tempo de resposta no acesso e períodos de indisponibilidade da internet e de sistemas críticos; incidentes de segurança, tais como vírus, *trojans*, furtos, acessos indevidos e outras ameaças; uso da capacidade instalada da rede e dos equipamentos; acesso à internet e aos sistemas críticos e atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet;

XII - estabelecer normas para uso da internet, intranet e correio eletrônico de forma a esclarecer servidores e colaboradores da JMU sobre quais são as atividades permitidas e proibidas quanto ao uso desses serviços, bem como cientificar que a utilização para fins pessoais é concessão e será permitida desde que feita com bom senso, não prejudique a imagem da instituição JMU e, também, não sobrecarregue o tráfego da rede;

XIII - estabelecer procedimentos para descarte e baixa do acervo magnético e digital.

Art. 23. Compete à Diretoria de Documentação e Gestão do Conhecimento (DIDOC):

I - estabelecer normas e procedimentos para proteção, reprodução, digitalização, manuseio, remoção, exposição, empréstimos, trânsito, guarda, conservação e restauração do acervo documental, museológico e bibliográfico da JMU em suporte físico;

II - designar o responsável por cada acervo de que trata o inciso I: em exposição, em circulação interna, em sala de consulta, em reserva técnica, em restauração, em empréstimo e em trânsito, dentro e fora da JMU;

III - estabelecer procedimentos para descarte e baixa do acervo físico;

IV - estabelecer e difundir as melhores práticas na área de produção, tramitação, classificação, preservação e arquivamento de documentos físicos.

SEÇÃO VII
DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO

Art. 24. Ao Comitê Gestor de Segurança da Informação (CGSI), além das atribuições já estabelecidas no art. 2º da Resolução STM nº 194, de 28 de agosto de 2013, compete:

I - definir planos, normas e procedimentos para credenciamento de segurança e de tratamento de informação classificada em qualquer grau de sigilo;

II - propor investimentos relacionados à segurança da Tecnologia da Informação e Comunicação (TIC) com a finalidade de minimizar e eliminar vulnerabilidades e comprometimentos às informações custodiadas na JMU;

III - definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação e Comunicação (PSIC) ou das normas de segurança da informação, emanadas pelas unidades da JMU;

IV - avaliar os incidentes de segurança e propor ações corretivas para assegurar a eficácia e a contínua pertinência da PSIC.

SEÇÃO VIII
DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Art. 25. Para garantir o cumprimento das regras estabelecidas na PSIC, bem como dos planos e normas subsequentes estabelecidas pelas unidades da JMU, o CGSI poderá:

I - implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou *wireless* e outros componentes da rede, resguardados o direito à privacidade e o sigilo da correspondência, na forma da lei;

II - utilizar os relatórios gerados pelos diversos sistemas de informação para identificar os usuários, os respectivos acessos efetuados e o material manipulado;

III - realizar, a qualquer tempo, inspeção física nas máquinas, aparelhos e demais equipamentos, fixos e móveis, de sua propriedade;

IV - instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso;

V - tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou processo administrativo.

SEÇÃO IX
DAS DISPOSIÇÕES FINAIS

Art. 26. As unidades da JMU e os custodiantes da informação proporão ao Comitê Gestor de Segurança da Informação, no prazo máximo de 180 (cento e oitenta) dias, contados a partir da publicação desta Resolução, seus respectivos Planos decorrentes da presente Política.

Art. 27. O acesso e a classificação das informações produzidas ou custodiadas pela JMU são os estabelecidos na regulamentação interna da Lei de Acesso à Informação.

Art. 28. As informações produzidas por usuários, no exercício de suas funções, são patrimônio intelectual da JMU e não cabe a seus criadores qualquer forma de direito autoral.

Parágrafo único. Quando as informações forem produzidas por terceiros para uso exclusivo da JMU, a obrigatoriedade do seu sigilo deve ser estabelecida em instrumento adequado.

Art. 29. As normas relacionadas à segurança da informação editadas pela JMU deverão observar as disposições estabelecidas nesta Resolução.

Art. 30. A inobservância dos dispositivos desta Resolução pode acarretar, isolada ou cumulativamente, nos termos da lei, sanções administrativas, civis ou penais.

Art. 31. Os casos omissos serão resolvidos pelo Ministro-Presidente.

Art. 32. Esta Resolução entra em vigor na data de sua publicação.

Sala de Sessões do Superior Tribunal Militar, em 3 de fevereiro de 2016.

Ministro Ten Brig Ar **WILLIAM DE OLIVEIRA BARROS**
Presidente