STM SUPERIOR TRIBUNAL MILITAR
DIDOC/COGES/LEGIS
Publicado no BJM nº 16,
de 26/04/2024

006732/23-00.039

PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR

RESOLUÇÃO Nº 350, DE 16 DE ABRIL DE 2024

Institui a Política de Segurança Cibernética da Justiça Militar da União.

O SUPERIOR TRIBUNAL MILITAR, no uso das atribuições legais e regimentais, e tendo em vista a decisão do Plenário, proferida na 3ª Sessão Administrativa Presencial, de 16 de abril de 2024, ao apreciar o Expediente Administrativo nº 14/2024,

CONSIDERANDO que é imprescindível garantir a segurança cibernética do ecossistema digital da Justiça Militar da União;

CONSIDERANDO a Resolução nº 396, do Conselho Nacional de Justiça (CNJ), de 7 de junho de 2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO os termos da Resolução nº 370, do Conselho Nacional de Justiça, de 22 de junho de 2021, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTICJUD);

CONSIDERANDO a Norma da Associação Brasileira de Normas Técnicas (ABNT): ABNT NBR ISO/IEC 27014:2021, que trata dos conceitos, objetivos e processos para a governança da segurança da informação, pela qual as organizações podem avaliar, direcionar, monitorar e comunicar as atividades relacionadas à segurança da informação dentro da organização;

CONSIDERANDO a Norma ABNT NBR ISO/IEC 27002:2022, que trata de princípios e diretrizes gerais para a Gestão da Segurança da Informação; e

CONSIDERANDO que os impactos financeiros, operacionais e de reputação, gerados pelos ataques cibernéticos, têm se tornado cada vez mais avançados e com alto potencial de prejuízo, podendo ser imediatos e significativos; e

CONSIDERANDO fundamental aprimorar a capacidade do Poder Judiciário de coordenar pessoas, desenvolver recursos e aperfeiçoar processos, visando minimizar danos e agilizar o restabelecimento da condição de normalidade, em caso de ocorrência de ataques cibernéticos de grande impacto;

R E S O L V E:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Resolução institui a Política de Segurança Cibernética (PSC) no âmbito da Justiça Militar da União (JMU).

§ 1º A Política de Segurança Cibernética será composta pelas Políticas:

I - de Capacitação e Fomento da Cultura da Segurança Cibernética (PCFCSC/JMU);

II - de Gestão de Ativos de Tecnologia da Informação e Comunicação (PGATIC/JMU); e

III - de Controle de Acesso Lógico (PCAL/JMU).

§ 2º As Políticas referidas no § 1º serão instituídas por Ato Normativo.

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

I - política de segurança cibernética (PSC): o documento formal que estabelece as diretrizes e as responsabilidades referentes à segurança cibernética;

II - segurança cibernética: ações voltadas para a segurança de operações, a fim de garantir que os sistemas de informação sejam capazes de resistir a eventos, no espaço cibernético, que possam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

III - segurança da informação: ações para viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

IV - TIC: é uma sigla para Tecnologia da Informação e Comunicação, referente ao conjunto de processos, *hardwares*, *softwares*, sistemas e funções de telecomunicações, que proporcionam a automação e sustentação de comunicação e processos das organizações;

V - CGovTIC: Comitê de Governança da Tecnologia da Informação e Comunicação ao qual compete estabelecer estratégias, indicadores e metas institucionais, aprovar planejamentos e orientar as iniciativas e investimentos tecnológicos dentro dos temas específicos da área de tecnologia da informação e segurança cibernética;

VI - recursos de tecnologia da informação e comunicação: para fins da segurança cibernética, consideram-se os equipamentos servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer *hardware* e *software* que compõem soluções e aplicações de TIC, e os recursos tecnológicos que necessitem de acesso à rede corporativa da JMU;

VII - Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética **(**ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VIII - usuário: indivíduo ou organização que utiliza ou trabalha com algum sistema, dispositivo ou serviço de TIC oferecido pela JMU;

IX - credencial de acesso: permissão concedida por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso de recursos tecnológicos;

X - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema, que também poderá ocorrer pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso;

XI - risco: evento incerto capaz de afetar positivamente ou negativamente os objetivos, processos de trabalho e iniciativas da JMU nos níveis estratégico, tático ou operacional, com sua medição em termos de impacto e de probabilidade; e

XII - unidade gestora de segurança cibernética: unidade responsável pela gestão da segurança cibernética no âmbito da Justiça Militar da União.

Art. 3º A Estratégia de Segurança Cibernética da Justiça Militar da União (ESEC-JMU) seguirá as diretrizes da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), estabelecidas pelo Conselho Nacional de Justiça (CNJ).

Art. 4º Integram a ESEC-JMU:

I - a Política de Segurança Cibernética (PSC);

II - as Normas de Segurança Cibernética, que devem contemplar as obrigações a serem seguidas de acordo com os objetivos e diretrizes estabelecidos nesta PSC; e

III - os Procedimentos de Segurança Cibernética, que definem regras operacionais de acordo com os Planos e as Normas de Segurança Cibernética.

Art. 5º A ESEC-JMU está baseada em 3 (três) níveis:

I - governança de segurança cibernética exercida pela Alta Administração, alinhada com o Planejamento Estratégico Institucional (PEI) e o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

II - gestão de segurança cibernética executada pela unidade de gestão de segurança cibernética, em conjunto com as áreas que utilizam os recursos e serviços de tecnologia da informação e comunicação de dados; e

III - supervisão das operações de segurança cibernética executadas pelas áreas operacionais de tecnologia da informação e comunicação de dados.

CAPÍTULO II
DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Seção I
Dos Princípios

Art. 6º A Política de Segurança Cibernética (PSC) da JMU tem como objetivo garantir os seguintes princípios básicos:

I - segurança jurídica;

II - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial: a liberdade de expressão, a proteção de dados pessoais, a proteção de privacidade e o acesso à informação;

III - visão abrangente e sistêmica da segurança cibernética;

IV - integração, cooperação e intercâmbio científico e tecnológico entre os órgãos da Administração Pública Federal e o meio acadêmico relacionado à segurança cibernética;

V - educação e inovação como alicerce fundamental para o fomento da cultura em segurança cibernética;

VI - orientação à gestão de riscos e à gestão da segurança cibernética;

VII - prevenção, tratamento e resposta a incidentes cibernéticos;

VIII - articulação entre as ações de segurança cibernética e de proteção de dados e ativos de informação; e

IX - garantia ao sigilo das informações imprescindíveis à segurança da sociedade e do Estado, e inviolabilidade da vida privada, da honra e da imagem das pessoas.

Seção II
Dos Objetivos

Art. 7º São objetivos da Política de Segurança Cibernética:

I - declarar formalmente o compromisso da JMU com a segurança cibernética;

II - dotar as unidades da Justiça Militar da União de instrumentos jurídicos, normativos e organizacionais que as capacitem de forma a assegurar os princípios básicos de segurança cibernética;

III - promover a conscientização e a capacitação de recursos humanos para o desenvolvimento de atividades, em consonância com as normas e procedimentos de segurança cibernética;

IV - promover o intercâmbio científico-tecnológico entre a JMU, as entidades do Poder Judiciário Nacional e as instituições públicas e privadas, sobre as atividades de segurança cibernética.

V - promover treinamento contínuo e certificação, inclusive internacional, dos profissionais diretamente envolvidos na área de segurança cibernética;

VI - estabelecer e aprimorar a estrutura normativa necessária à efetiva implementação da segurança cibernética;

VII - promover as ações necessárias à implementação e à manutenção dos processos de gestão da segurança cibernética;

VIII - fortalecer a cultura de segurança cibernética no âmbito da JMU; e

IX - orientar ações relacionadas:

a) à gestão em segurança cibernética;

b) à segurança das infraestruturas críticas;

c) ao tratamento das informações;

d) à prevenção, ao tratamento e à resposta a incidentes cibernéticos;

e) à gestão e operação de equipe de tratamento e resposta a incidentes cibernéticos (ETIR);

f) ao estabelecimento dos níveis de maturidade em segurança cibernética;

g) ao estabelecimento de processo transparente de comunicação e respostas a incidentes cibernéticos entre o poder público e a sociedade; e

h) ao estabelecimento de requisitos mínimos de segurança cibernética nas contratações e nos acordos que envolvam a comunicação com outros órgãos.

Seção III
Das Diretrizes

Art. 8º São diretrizes da Política de Segurança Cibernética:

I - a promoção do uso adequado dos recursos de tecnologia da informação e comunicação, visando garantir a continuidade da prestação jurisdicional e administrativa da JMU;

II - a utilização dos recursos de tecnologia da informação e comunicação disponibilizados, exclusivamente em atividades relacionadas às funções institucionais;

III - a monitoração dos recursos de tecnologia da informação e comunicação utilizados, sendo seus registros mantidos pela Diretoria de Tecnologia da Informação (DITIN);

IV - a informação produzida ou recebida no âmbito da JMU pertence ao próprio órgão. Explicitar e formalizar as exceções entre as partes;

V - as informações devem ser classificadas e protegidas de acordo com o nível de confidencialidade exigido pelas atividades da JMU;

VI - o acesso à informação, independentemente da forma ou meio de exibição e de compartilhamento, deverá ser protegido adequadamente, de acordo com os controles definidos pela Política de Segurança da Informação da JMU e documentos complementares;

VII - o controle de acesso deverá considerar e respeitar o princípio do privilégio mínimo, para configurar as credenciais ou permissões de acesso dos usuários aos ativos de informação da JMU;

VIII - a garantia da continuidade dos serviços prestados pela JMU em caso de acidentes ou falhas graves na sua operação; e

IX - o cumprimento da PSC, das normas, dos procedimentos de segurança cibernética e de outros dispositivos legais pertinentes serão acompanhados pelo (CGovTIC).

Art. 9º O tratamento de dados pessoais deverá estabelecer as diretrizes no âmbito da JMU em regulamentação específica, em conformidade com a Lei n.º 13.709/2018 (LGPD).

Seção IV
Das Responsabilidades

Art. 10. São responsabilidades dos usuários:

I - conhecer e cumprir esta PSC e suas normas e procedimentos complementares;

II - seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e informacionais do órgão;

III - utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da JMU;

VI - zelar pelas suas credenciais de acesso, de uso pessoal e intransferível, vedada sua divulgação a terceiros;

VII - manter-se atualizado sobre esta PSC, normas e procedimentos relacionados, buscando informação junto à DITIN quando não estiver seguro quanto à obtenção, uso e/ou descarte de informações; e

VIII - comunicar à DITIN quaisquer ocorrências ou suspeitas de incidentes de segurança cibernética.

Art. 11. São responsabilidades do CGovTIC:

I - direção: direcionar os objetivos e as estratégias de segurança cibernética que devem ser implementados, priorizando recursos e atividades;

II - avaliação: averiguar os objetivos de segurança cibernética atingidos e previstos e determinar eventuais ajustes para atingir objetivos estratégicos;

III - monitoração: avaliar a eficácia das atividades de gestão de segurança cibernética com o objetivo de verificar o alcance dos objetivos estratégicos definidos; e

IV - comunicação: processo bidirecional, o corpo diretivo e órgãos externos, ou em última instância, com a própria sociedade, trocam informações sobre a segurança cibernética.

Art. 12. São responsabilidades da DITIN:

I - apoiar o CGovTIC na conscientização e orientação dos usuários em relação à PSC e suas normas e procedimentos complementares;

II - implementar os controles tecnológicos necessários para garantir o cumprimento dos procedimentos, normas e Política de Segurança Cibernética;

III - analisar e tratar os incidentes de segurança cibernética e propor as medidas cabíveis;

IV - propor programas destinados à formação e ao aprimoramento das equipes especializadas nos campos da segurança cibernética; e

V - acompanhar a evolução do conhecimento em segurança cibernética por meio de relatórios enviados pela unidade de gestão da segurança cibernética.

Art. 13. São responsabilidades da unidade de gestão da segurança cibernética:

I - coordenar as ações de análise, avaliação e tratamento de riscos de segurança cibernética a serem executadas pelas áreas operacionais e a Equipe de Tratamento de Incidentes;

II - elaborar relatórios cujo conteúdo constará a análise das ações realizadas com os resultados obtidos e a consequente proposição de ajustes e de medidas preventivas e proativas à DITIN;

III - propor o plano de segurança cibernética contendo as ações que serão incorporadas no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);

IV - propor à DITIN cursos e treinamentos com o cronograma de ações de capacitação e de conscientização voltadas ao órgão, de acordo com as características de cada público destinatário; e

V - gerenciar os processos de segurança cibernética, os normativos e os protocolos para o tratamento de incidentes.

CAPÍTULO III
DAS DISPOSIÇÕES FINAIS

Art. 14. O descumprimento das disposições desta Resolução sobre PSC ou de suas normas e procedimentos complementares, sujeitam o infrator às penalidades previstas na legislação e nos regulamentos internos da JMU.

Parágrafo único. A inobservância da PSC poderá configurar infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo das responsabilidades penal e cível.

Art. 15. Os casos omissos serão resolvidos pelo CGovTIC.

Art. 16. Fica revogada a Resolução nº 298, de 04 de agosto de 2021.

Art. 17. Esta Resolução entra em vigor na data de sua publicação.

Ten Brig Ar **FRANCISCO JOSELI PARENTE CAMELO**
Ministro-Presidente

Documento assinado eletronicamente por **FRANCISCO JOSELI PARENTE CAMELO**, **MINISTRO-PRESIDENTE DO SUPERIOR TRIBUNAL MILITAR**, em 22/04/2024, às 18:45 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **3707077** e o código CRC **72A4CCF4**.

3707077v6