ESTADO DE MATO GROSSO
PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA

RESOLUÇÃO TJMT/OE Nº 17 DE 28 DE JULHO DE 2022.

Dispõe sobre a Política de Segurança da Informação e Comunicação (POSIC) do Poder Judiciário do Estado de Mato Grosso.

A PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DE MATO GROSSO, no uso de suas atribuições legais e regimentais e, em conformidade com a deliberação do Egrégio Órgão Especial, na sessão administrativa realizada em 28/07/2022, nos autos da Proposição n. 9/2021 (Cia 0045075-84.2020.8.11.0000),

RESOLVE:

Art. 1º. Reformular a Política de Segurança da Informação e Comunicação (POSIC) no âmbito do Poder Judiciário do Estado de Mato Grosso a qual passa a ser regida nos seguintes termos:

Seção I
Das Definições Relativas à POSIC

Art. 2º. Para efeitos desta Política ficam estabelecidos as seguintes denominações:

I – ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a confidencialidade, a integridade, a autenticidade e/ou disponibilidade da informação;

II – ativos de tecnologia da informação e comunicação ou Ativo de TIC: São todos os elementos relacionados à tecnologia da informação que possuem relevância para a continuidade de serviços e atividades de negócio. Podem ser tanto informações na forma de documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, logs de sistemas, planos, guias e etc., quantos programas de computador (*softwares*) ou equipamentos (computadores de mesa ou portáteis, dispositivos de infraestrutura de

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53

processamento ou armazenamento de dados, componentes de redes, cabos, etc.). Podem ser ainda serviços tais como links de comunicação, serviços de suporte ou direitos de uso estabelecidos em contratos. Podem ainda ser mídias como CD-ROMs, *tokens*, HDs externos etc.;

III – autenticidade: é a garantia de que a informação é proveniente da fonte anunciada e que não foi alvo de mutações indevidas ao longo de um processo;

IV – confidencialidade: é a garantia de que a informação seja acessível apenas àqueles autorizados a ter acesso;

V – disponibilidade: é a garantia de que a informação esteja acessível e utilizável, por indivíduos, entidades ou processos;

VI – incidente de segurança: evento ou conjunto de eventos indesejados confirmados que causem impacto negativo sobre a confidencialidade, a integridade, a autenticidade e/ou a disponibilidade da informação;

VII – integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos;

VIII – risco: possibilidade potencial de uma ameaça comprometer a informação ou o sistema de informação pela exploração da vulnerabilidade;

IX – risco residual: é a parcela do risco que permanece mesmo após a adoção das medidas mitigatórias (resposta) possíveis;

X – vulnerabilidade: fragilidade de um ativo ou grupo de ativos de informação que pode ser explorado negativamente por uma ou mais ameaças;

XI – serviços essenciais de TIC: são as soluções de tecnologia da informação e comunicação indispensáveis à continuidade da prestação jurisdicional ou das atividades administrativas imprescindíveis à manutenção do funcionamento do Poder Judiciário do Estado de Mato Grosso;

XII – ETIR – Equipe de Tratamento e Respostas a Incidentes de Segurança da Informação: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades de tratamento e respostas a incidentes de Segurança da Informação, a fim de contribuir para a garantia da disponibilidade, integridade e confidencialidade das informações.

Seção II

Da Gestão de Ativos de Tecnologia da Informação e Comunicação

Art. 3º. As ações e controles específicos de segurança deverão garantir a proteção adequada dos ativos de TIC do Poder Judiciário do Estado de Mato Grosso, em níveis compatíveis ao seu grau de importância e alinhados aos objetivos estratégicos do órgão.

Art. 4º. A Presidência do Tribunal de Justiça, com orientação do Comitê Gestor de Segurança da Informação (CGSI), deverá instituir normas e procedimentos que

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53

garantam a adequada gestão dos ativos de TIC inventariados no âmbito do Poder Judiciário do Estado de Mato Grosso, compondo uma Política de Gestão de Ativos de Tecnologia da Informação que estabeleça no mínimo:

I – sistemas de proteção mínimos obrigatórios aplicáveis a cada ativo;

II – regras de controle do ciclo de vida dos ativos;

III – regras de uso para os ativos de TIC.

Parágrafo único. Os ativos de TIC serão inventariados de forma paulatina e progressiva, priorizados conforme sua essencialidade para a preservação da segurança das informações e dos serviços de TIC.

Seção III
Do Controle de Acesso

Art. 5º. A Presidência do Tribunal de Justiça, com orientação do Comitê Gestor de Segurança da Informação, deverá instituir uma política de controle de acesso, contendo diretrizes, procedimentos e regras para conceder ou bloquear o acesso físico e lógico, à infraestrutura de TIC e aos serviços de TIC do Poder Judiciário do Estado de Mato Grosso, estabelecendo no mínimo:

I – padrões de autenticação e autorização de credenciais de acesso dos usuários e sistemas;

II – regras para concessão ou bloqueio de acesso lógico à infraestrutura de TIC e aos serviços de TIC;

III – regras para utilização das credenciais de acesso;

IV – meios de ampla e recorrente divulgação das regras de uso estabelecidas;

V – critérios de aceitação formal e explícita das regras de uso pelos usuários, na forma de Termos de Uso ou assemelhados.

Art. 6º. Estão sujeitos à regulamentação de que trata o caput do art. 5º os usuários internos e externos do Poder Judiciário do Estado de Mato Grosso que, de maneira autorizada, tenham acesso aos recursos de Tecnologia da Informação prestados por este Poder Judiciário.

Seção IV
Da Segurança das Comunicações

Art. 7º. A Presidência do Tribunal de Justiça, com orientação do Comitê Gestor de Segurança da Informação, deverá instituir normas e procedimentos que garantam a segurança das comunicações na rede corporativa do Poder Judiciário do Estado de Mato Grosso, compondo uma Política de Segurança das Comunicações que estabeleçam no mínimo:

I – diretrizes para segregação lógica da rede corporativa visando à preservação

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53

da rede interna;

II – regramento para troca de mensagens eletrônicas como e-mail, SMS, serviços de mensageria instantânea, serviços de interoperabilidade entre sistemas, entre outras;

III – regramento padrão para o acesso à internet no âmbito do PJMT;

IV – meios de ampla e recorrente divulgação da política estabelecida.

Seção V
Da Gestão de Incidentes de Segurança da Informação

Art. 8º. Os incidentes de segurança da informação serão geridos de modo sistemático, por meio de processos de trabalho estruturados e controlados, garantindo seu registro, classificação e tratamento pela Coordenadoria de Tecnologia da Informação, utilizando-se preferencialmente de seus canais eletrônicos.

Art. 9º. A gestão dos incidentes será balizada pelos Protocolos e Manuais de referência estabelecidos na ENSEC (Resolução 396/2021) do CNJ listados abaixo:

I – o Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário (PPINC-PJ);

II – o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Poder Judiciário (PPINC-PJ);

III – o Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário (PIILC-PJ);

IV – manual de Proteção de Infraestruturas Críticas de TIC;

V – manual de Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;

VI – manual de Gestão de Identidades; e

VII – manual de Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.

Art. 10. A adoção dos protocolos e manuais preconizados pelo Conselho Nacional de Justiça ocorrerá de forma paulatina em ciclos de aprimoramento, de acordo com a viabilização de recursos técnicos e operacionais para sua execução, cabendo ao Comitê de Segurança da Informação a elaboração e acompanhamento dos planos de ação para aderência às práticas.

Art. 11. A Presidência do TJMT deverá emitir normas complementares para adaptação dos protocolos e manuais da ENSEC às necessidades do PJMT, incluindo, no mínimo:

I – instituição da equipe ETIR, discriminando sua composição, atribuições, autonomia, procedimentos e deveres de comunicação, no prazo de 30 dias;

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53

II – instituição do Comitê de Crises Cibernéticas discriminando sua composição e atribuições, no prazo de 30 dias.

Seção VI
Da Continuidade dos Serviços Essenciais de TIC

Art. 12. Caberá à Coordenadoria de Tecnologia da Informação, elaborar um Plano de Continuidade e de Recuperação dos Serviços Essenciais de TIC visando estabelecer procedimentos para garantir a não interrupção de serviços de TIC e sua eventual recuperação em casos de desastres, contendo no mínimo:

a) relação dos serviços essenciais de TIC, ordenados por relevância para a prestação jurisdicional e serviços administrativos indispensáveis a este;

b) relação da infraestrutura básica de TIC para operacionalização e recuperação dos serviços;

c) descrição das estratégias de mitigação de riscos e procedimentos de continuidade de serviços judiciais, administrativos e de suporte técnico;

d) mapeamento de riscos residuais referentes à Infraestrutura básica de TIC;

e) procedimentos de recuperação em desastre.

Art. 13. O Plano de Continuidade e de Recuperação dos Serviços Essenciais de TIC será submetido ao Comitê Gestor de Segurança da Informação e ao Comitê de Governança de Tecnologia da Informação e Comunicação, com posterior encaminhamento à Presidência do Tribunal de Justiça do Estado de Mato Grosso.

Art. 14. O Plano de Continuidade e de Recuperação dos Serviços Essenciais de Tecnologia da Informação será testado pela Coordenadoria Tecnologia da Informação e os resultados documentados de forma a garantir a sua efetividade, com encaminhamento subsequente ao Comitê Gestor de Segurança da Informação.

Parágrafo único. Fica dispensada a execução dos testes estabelecidos no *caput* deste artigo quando os riscos residuais para sua realização ainda forem relevantes.

Art. 15. O Plano de Continuidade e de Recuperação de Serviços Essenciais de Tecnologia da Informação será revisado nas seguintes situações:

I – no mínimo, a cada dois anos;

II – em função dos resultados dos testes realizados;

III – mediante solicitação do Comitê Gestor de Segurança da Informação ou do Comitê Gestor de Tecnologia da Informação e Comunicação.

Seção VII
Da Segurança de Desenvolvimento de Sistemas

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53

Art. 16. A Presidência do Tribunal de Justiça do Estado de Mato Grosso, com orientação do Comitê Gestor de Segurança da Informação, deverá instituir normas e procedimentos que garantam a segurança dos sistemas de informação desenvolvidos ou mantidos pelo Poder Judiciário do Estado de Mato Grosso, compondo uma Política de Segurança de Desenvolvimento de Sistemas que estabeleça no mínimo:

a) padronização tecnológica;

b) controle sobre os códigos fontes;

c) segregação do ambiente de produção, dos demais locais de confecção e validação dos sistemas: de teste, de homologação e de treinamento, etc.;

d) segregação de permissões, no mínimo, entre os ambientes de desenvolvimento e produção;

e) padronização de mecanismos de autenticação e autorização para usuários;

f) processo de controle de publicações de versões que garanta os níveis de autorização adequados;

g) avaliação de impacto nos dados pessoais.

Art. 17. Os instrumentos de contratação e/ou suporte a sistemas de informação utilizados pelo PJMT, deverão considerar a obrigatoriedade da contratada em prover a correção de vulnerabilidades que venham a ser identificadas em sua solução.

Seção VIII

Das Disposições Finais

Art. 18. O Comitê Gestor de Segurança Cibernética e da Informação poderá propor à Presidência normas complementares para instrumentalizar as disposições desta Resolução.

Art. 19. O Comitê Gestor de Segurança Cibernética e da Informação deverá reportar semestralmente ao Comitê de Governança de Tecnologia da Informação e Comunicação – CGoTIC e à Presidência do Tribunal de Justiça as ações relevantes de segurança e informações ão e gerenciais executivas.

Art. 20. Os instrumentos normativos complementares estabelecidos nos artigos 4º, 5º, 7º, 11, 12 e 16, serão editados por atos da Presidência, passando a fazer parte integrante da Política de Segurança da Informação do Poder Judiciário do Estado de Mato Grosso estabelecida por esta Resolução.

§ 1º. As políticas complementares de Gestão de Ativos de Tecnologia da Informação, Política de Segurança nas Comunicações e Plano de Continuidade e de Recuperação dos Serviços Essenciais de TIC, Política de Acessos e Uso de Recurso de TIC e Política de Segurança de Desenvolvimento de Sistemas, serão editadas no prazo máximo de 30 (trinta) dias da publicação desta Resolução.

§ 2º. Até que sejam editadas as políticas complementares descritas no parágrafo anterior, as questões por ela tratadas continuarão disciplinadas, no que for aplicável, pelas disposições constantes da Resolução n. 11/2013-TP.

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53

Art. 21. Os casos omissos na presente Resolução serão resolvidos pelo Comitê Gestor de Segurança da Informação do Poder Judiciário do Estado de Mato Grosso.

Art. 22. Esta Resolução entra em vigor 30 dias após a publicação, ficando revogada a Resolução 11/2013/TP e eventuais disposições contrárias.

Desembargadora MARIA HELENA GARGAGLIONE PÓVOAS

Documento assinado digitalmente por: Maria Helena Gargaglione Póvoas
Para ValidarFormularioAssedio a(s) assinatura(s) ou baixar o original acesse https://cia.tjmt.jus.br/publico/ValidarDocumento e utilize o código 78654B53