RESOLUÇÃO N.º 06, DE 02 DE MARÇO DE 2016.

Dispõe sobre a Política de Segurança da Informação do Tribunal de Justiça do Estado de Roraima.

O EGRÉGIO TRIBUNAL DE JUSTIÇA DO ESTADO DE RORAIMA, em sua composição plenária, no uso de suas atribuições legais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias ao funcionamento deste Tribunal com integridade, confidencialidade, disponibilidade e confiabilidade;

CONSIDERANDO que o Tribunal de Justiça do Estado de Roraima, no exercício de suas competências, gera, adquire e absorve informações, que devem permanecer íntegras, disponíveis e, quando for o caso, com o sigilo resguardado;

CONSIDERANDO que a integridade e a credibilidade da instituição na prestação jurisdicional devem ser preservadas;

CONSIDERANDO a constante preocupação com a qualidade e celeridade na prestação de serviços à sociedade.

CONSIDERANDO que as informações no TJRR são armazenadas em diferentes meios, veiculadas por diferentes formas, manuseadas e tratadas por diversas pessoas e entidades e, portanto, vulneráveis aos incidentes em segurança da informação;

CONSIDERANDO que a adequada gestão da informação precisa nortear todos os processos de trabalho e deve ser impulsionada por uma Política de Segurança da Informação;

RESOLVE:

Art. 1º. Instituir a Política de Segurança da Informação (PSI) do Tribunal de Justiça do Estado de Roraima (TJRR).

CAPÍTULO I
VISÃO GERAL E GLOSSÁRIO

Art. 2º. A Política de Segurança da Informação (PSI) do TJRR e de seus órgãos acessórios é uma declaração de compromisso com a proteção das informações que cria, manipula, custódia ou que são de sua propriedade, sob o gerenciamento de sua infraestrutura de Tecnologia da Informação e

Comunicação (TIC), devendo ser conhecida, compreendida e cumprida por todos que tenham acesso às informações.

Parágrafo único. A utilização dos recursos e dispositivos de Tecnologia da Informação e Comunicação (TIC) do TJRR, ou pessoais em seu proveito, deve ser pautada pelos princípios da ética, segurança e legalidade.

Art. 3º. A Comissão de Segurança da Informação (CSI) publicará, via portaria, glossário específico, o que conterá denominações e limitará conceitos que se aplicarão à PSI, suas normas e procedimentos correlatos, de indispensável conhecimento pelos agentes judiciários ou terceiros interessados que tiverem contato com informações e demais recursos de TIC.

CAPÍTULO II
ESTRUTURA NORMATIVA, APROVAÇÃO E REVISÃO

Art. 4º. A Estrutura Normativa da Segurança da Informação – ENSI do TJRR é composta pelos seguintes documentos, hierarquicamente organizados, com a indicação de seus respectivos responsáveis por aprovação e periodicidade de revisão:

Política de Segurança da Informação (PSI): consiste em diretrizes gerais e princípios básicos, com a finalidade de nortear todas as ações que garantirão a manutenção da Segurança da Informação. A Política e suas revisões serão aprovadas pelo Tribunal Pleno do TJRR, com periodicidade de revisão bienal ou conforme a necessidade;

Normas de Segurança da Informação: estabelecem os controles, os métodos, as restrições e as responsabilidades para atendimento à PSI. As normas e suas revisões serão aprovadas pela CSI , com periodicidade de revisão anual ou conforme necessidade;

Procedimentos de Segurança da Informação: definem como as operações de atendimento à PSI e normas correlatas devem ser realizados. Os procedimentos e suas revisões serão propostos pela STI, com periodicidade de revisão anual ou conforme a necessidade, e aprovados pela CSI.

Art. 5º. Também compõem a ENSI outros documentos acessórios, a saber: termos e acordos de responsabilidade e confidencialidade perante quem tomar contato com informações do Poder Judiciário do Estado de Roraima.

CAPÍTULO III
REQUISITOS DE CAPITAL HUMANO, SUAS OBRIGAÇÕES E RESPONSABILIDADES

Art. 6º. Para os efeitos desta Política entende-se por classes de agentes do Judiciário: magistrados, servidores efetivos, servidores cedidos, servidores comissionados, estagiários, voluntários e terceirizados.

Art. 7º. Cabe aos agentes do Judiciário:

I - Firmar, obrigatoriamente, Termo de Responsabilidade e Confidencialidade sobre as informações;
II - Participar das campanhas, eventos ou atualizações promovidas sobre Segurança da Informação no âmbito do TJRR;
III - Estar sempre atualizado e ciente das políticas, normas e procedimentos vigentes do TJRR ou do órgão subordinado que executar suas tarefas;
IV - Cumprir o disposto nos documentos da ENSI do TJRR;
V - Utilizar, modificar ou reproduzir dados e informações do TJRR exclusivamente para o desempenho de suas funções, da mesma forma que a utilização dos dispositivos de TIC em nome do TJRR;
VI - Não divulgar, compartilhar, transmitir ou deixar-se conhecer informações a pessoas que não tenham nível de autorização suficiente;
VII - Não divulgar, compartilhar, transmitir, veicular ou permitir a divulgação, por qualquer meio, informações sobre ativos ou de procedimentos do TJRR, exceto quando houver autorização prévia e formal por superior hierárquico ou de acordo com a legislação vigente para tanto;
VIII - Não conduzir, transportar, enviar, transmitir, compartilhar ou deixar que dados e informações alcancem ambiente ou destinatário fora das dependências ou controle do Tribunal sem autorização formal;
IX - Proteger ativos de informação contra acesso, divulgação, transmissão, compartilhamento, modificação, destruição ou interferência não autorizadas;
X - Estar atento ao repassar ou transmitir informações para outras pessoas, seja de forma presencial, via telefone, comunicadores instantâneos, mensagens eletrônicas ou mídias sociais. Confirmar a identidade e idoneidade do solicitante ou destinatário antes do envio de informações e, sempre que possível, a real necessidade do compartilhamento de alguma informação solicitada por outra pessoa, mesmo que de sua confiança;
XI - Reportar à Comissão de Segurança da Informação, quaisquer eventos ou incidentes potenciais ou reais que causem riscos à segurança das informações do TJRR, ou ainda sua mera suspeita.

Art. 8º. Cabe aos magistrados e chefias:

I - Conhecer, divulgar, cumprir e estimular o cumprimento da PSI, normas e procedimentos correlatos;
II - Atribuir o perfil adequado para acesso a recursos, dados e informações conforme a necessidade, com base nos princípios do conjunto mínimo de permissões que precisam ser atribuídos;
III - A responsabilidade por gerir os recursos de TIC e postura dos agentes

judiciários que compõem sua área ou equipe em relação à Segurança da Informação.

Art. 9º. Cabe à Comissão de Segurança da Informação:
I - Propor alterações na Política de Segurança da Informação (PSI);
II - Elaborar e promover alterações das Normas de Segurança da Informação, sempre que pertinente;
III - Propor alterações e aprovar os termos acessórios da PSI;
IV - Analisar os casos de violação da PSI, incidentes, vulnerabilidades e tentativas de burla, encaminhando-os à Presidência do TJRR, quando providências a serem autorizadas por esta forem requeridas;
V - Propor medidas relacionadas à melhoria da Segurança da Informação do TJRR;
VI - Propor o planejamento e a alocação de recursos no que tange à Segurança da Informação do TJRR;
VII - Aprovar a relação de responsáveis pelas informações pertencentes ou sob a guarda do TJRR;
VIII - Aprovar ou reprovar o acesso a locais de rede, sítios de internet, uso de dispositivos de TIC pessoais no ambiente da instituição e demais regras de uso dos recursos de TIC oferecidos pelo TJRR aos agentes do judiciário.
IX - Publicar e manter atualizado o Glossário da PSI, referido no art. 3º da presente Resolução, sempre que se fizer necessário.

Art. 10. Cabe à Secretaria de Tecnologia da Informação (STI):

I - Emitir, revogar ou suspender as credenciais de acesso, sempre que solicitadas pela SDGP.
II - Manter registros de atividades dos usuários pelo tempo correspondente na tabela de temporalidade em vigor, permitindo controles e auditorias;
III - Formalizar orientação para a SDGP nas políticas adequadas e aplicáveis aos usuários, cargos, funções e lotação, sempre que necessário;
IV - Apoiar as campanhas de conscientização de Segurança da Informação fornecendo os recursos de TIC necessários;
V - Fomentar, sempre que possível, sistema de login unificado/centralizado para acesso aos diversos sistemas.
VI - Para os sistemas desenvolvidos internamente ou cujo desenvolvimento é mantido pela própria equipe do TJRR, o login unificado é mandatório e deve ser implementado no prazo máximo de 24 (vinte quatro) meses a partir da data de publicação desta resolução.
VII - Para os sistemas contratados, mantidos ou desenvolvidos por terceiros que já estejam em uso pelo TJRR, deverão ser promovidos esforços para que venham se adequar ao sistema de login unificado.
VIII - Para novos sistemas que venham a ser contratados de terceiros ou desenvolvidos internamente, o login unificado passa a ser pré-requisito elementar, a menos que a possibilidade de login unificado semostre inviável.

IX - Implantar no prazo máximo de 24 (vinte quatro) meses processo de login através de certificado digital.
X - Promover campanhas com o objetivo de conscientizar os agentes judiciários sobre a ENSI;
XI - Fomentar ações para implementar as diretrizes previstas na PSI, normas e procedimentos correlatos;
XII - Reportar imediatamente à STI os eventos que violem, ou tentem violar, os termos da PSI, das normas ou procedimentos correlatos, ainda que por mera suspeita;
XIII - Promover a criação e manutenção de diretrizes, princípios e conteúdos da ENSI;
XIV - Solicitar a revogação ou suspensão das credenciais de acesso sempre que detectar a utilização inadequada das mesmas ou a reativação, conforme o caso;
XV - Coordenar a elaboração, manutenção, implementação e testes do plano de continuidade do negócio e prevenção a desastres;
XVI - Zelar para que as diretrizes e os princípios desta política sejam respeitados, informando de ofício, os incidentes e ações à STI, ainda que por mera suspeita;
XVII - Responder, adequadamente, a quaisquer consultas das outras áreas sobre a aplicação da PSI, normas e procedimentos de Segurança da Informação e uso aceitável da infraestrutura de tecnologia e comunicação, orientando-as sobre as melhores práticas;
XVIII - Aprovar, reprovar, suspender ou promover a homologação de softwares e hardwares para o uso dos agentes judiciários e divulgar lista com permissões e proibições que julgar pertinente;
XIX - Aprovar, reprovar, suspender ou promover a liberação do uso de dispositivos de TIC pessoais dos agentes judiciários no ambiente institucional e aplicar as medidas de segurança cabíveis para a preservação da infraestrutura de TIC do TJRR;
XX - Aprovar e publicar a PSI, suas revisões e documentos acessórios.

Art. 11. Cabe à Secretaria de Desenvolvimento e Gestão de Pessoas (SDGP) quanto aos servidores e magistrados:

I - Manter atualizados, no sistema informatizado de gestão de pessoas, todos os dados referentes a desligamentos, afastamentos, retornos e modificações no quadro funcional do TJRR e de seus órgãos subordinados. Da mesma forma, manter o status atualizado das credenciais que precisem ser emitidas, revogadas e suspensas;
II - Apoiar as campanhas de conscientização de Segurança da Informação, em parceria com a STI;
III - Incluir o Termo de Responsabilidade e Confidencialidade como documento obrigatório para exercício dos agentes do Judiciário e proceder à guarda segura e adequada dos documentos assinados, conforme estabelecido pela

tabela de temporalidade vigente.

CAPÍTULO IV
CLASSIFICAÇÃO DA INFORMAÇÃO, CONTROLE E CREDENCIAIS DE ACESSO

Art. 12. Cabe aos responsáveis pela informação a classificação e a definição de quem possui acesso e o tipo de privilégios de acesso, sem prejuízo do disposto na legislação vigente.

Art. 13. Os agentes judiciários têm o dever de cumprir com o nível de segurança exigido pela classificação das informações, sob pena de responsabilidade (substituir todos os casos) conforme a gravidade do ato e os prejuízos sofridos.

Art. 14. Não é permitido o acesso ou uso de qualquer recurso de TIC ou ativo da informação sem as credenciais de acesso correspondentes.

Art. 15. O agente judiciário deve proteger sua identidade digital, devendo suas credenciais, senhas e acessos serem pessoais e tratados de forma segura, confidencial, intransferível, intransmissível, possuindo apenas as permissões suficientes para realização da s suas atividades, com orientação nos princípios do conjunto mínimo de permissões que precisam ser atribuídos.

Art. 16. O acesso aos ambientes físicos e recursos lógicos de TIC devem ser controlados e restritos às pessoas autorizadas pela STI, conforme orientação do binômio de necessidade funcional e mais restrita permissão cabível.

Art. 17. Todas as informações criadas, acessadas, compartilhadas, manuseadas, armazenadas ou disponibilizadas ao agente judiciário ou das quais tiver acesso no exercício de suas atividades, são de propriedade e/ou direito de uso exclusivo do TJRR.

Parágrafo único. Todos os ativos e informações do TJRR devem ser utilizados apenas para o cumprimento das atividades profissionais, dentro do padrão de conduta ética estabelecida pela ENSI do TJRR e às demais leis em vigor, respeitando os requisitos de sigilo profissional.

CAPÍTULO V
AQUISIÇÃO, UTILIZAÇÃO, CONTROLE E DESCARTE DE RECURSOS DE TIC

Aquisição

Art. 18. Para adquirir qualquer solução ou serviço de TI, a equipe de elaboração dos Estudos Preliminares deve considerar os requisitos legais,

resoluções internas e questões relacionadas com a garantia da segurança das informações que serão tratadas pela solução ou serviço.

Utilização

Art. 19. Os recursos de TIC de propriedade do TJRR somente poderão ser utilizados pelos agentes do judiciário.

Parágrafo único. Os Órgãos essenciais à Justiça somente poderão fazer uso dos recursos se forem previamente autorizados, por mecanismo formal, pela Secretaria Geral do TJRR, levando em consideração quaisquer responsabilidades legais na concessão.

Art. 20. Todos os equipamentos, dispositivos e demais recursos que fizerem uso da infraestrutura de TIC do TJRR estarão sujeitos à PSI e às demais normas de Segurança da Informação do TJRR e deverão possuir softwares de proteção instalados, a exemplo, mas não se limitando, de antivírus, anti-spyware e firewall sempre ativos e atualizados.

Art. 21. É permitido o uso de dispositivos pessoais de TIC nos ambientes do TJRR, desde que não haja restrição conforme seu perfil profissional e que não traga prejuízos para o TJRR, sendo vedado o uso da infraestrutura de TIC do TJRR a partir de dispositivos pessoais, a menos que seja previamente autorizado e cadastrado para uso pela STI.

§1º. Os agentes judiciários serão integralmente responsáveis pelos conteúdos armazenados em seus dispositivos pessoais e pelos atos através deles praticados, sem ressalvas ou exceções.

§2º. Os agentes judiciários poderão utilizar seus dispositivos pessoais de TIC durante o expediente profissional, isto é, desde que não atrapalhe a própria concentração ou dos demais a seu redor nas atividades que devem desempenhar, não prejudique o atendimento ao público ou atrase as tarefas que lhe cabem, não violem a ENSI ou gerem riscos ao TJRR, sob pena de responsabilidade.

Controle

Art. 22. São direitos do TJRR, através da STI, registrar, bloquear, permitir, suspender e limitar o uso dos recursos e dispositivos que compõem sua infraestrutura de TIC.

Art. 23. O TJRR, por meio da STI, monitora todos os recursos, ambientes, dispositivos e ativos ligados à Tecnologia de Informação e Comunicação, tais como, mas não se restringindo, o e-mail institucional, acesso à internet, estrutura de comunicação telefônica, espaços físicos e utilização dos dispositivos de TIC institucionais, com a finalidade de proteger seus ativos, sua

reputação e conhecimento.

§1º. O TJRR também registra todos os dados obtidos pelo monitoramento realizado para eventual análise forense, apuração a violações à Estrutura Normativa de Segurança de Informação, podendo investigar fatos que comprometam seus ativos.

§2º. Da mesma forma que indicado no caput, o TJRR possui a prerrogativa de registrar, inspecionar, apreender, isolar ou neutralizar dispositivos ou recursos de TIC de propriedade de terceiros que pretendam adentrar em seu perímetro lógico ou físico, ou até mesmo impedir que estes o façam, com a utilização das medidas de contenção que entender cabíveis para preservar a incolumidade de sua estrutura de TIC e pelo tempo que for necessário, observando os princípios de transparência, proporcionalidade e razoabilidade.

Descarte

Art. 24. O descarte de informações e ativos de TIC do TJRR devem ser realizados de forma segura, com a destruição, sanitização ou inutilização da mídia ou dispositivo que contém as informações, de modo que fique incapacitada de ser recuperada, adquirida ou reutilizada por terceiros.

CAPÍTULO VI
DESENVOLVIMENTO, AQUISIÇÃO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO

Art. 25. Os Sistemas de Informação adquiridos, mantidos ou desenvolvidos pelo TJRR deverão atender aos princípios e requisitos de Segurança da Informação, estabelecidos pela presente Resolução e demais normas em vigor.

Art. 26. As atividades de desenvolvimento, teste e homologação dos Sistemas de Informação não devem afetar o funcionamento dos sistemas em operação. Para isso, a STI deve manter ambientes de desenvolvimento, homologação e produção separados logicamente.

Art. 27. Os dados classificados como sigilosos, mantidos pelos Sistemas de Informação, não deverão estar replicados ou acessíveis em outro ambiente, sem a competente autorização da STI, sob o risco de vazamento de informações pessoais ou confidenciais sob a guarda do TJRR.

Parágrafo único. O descumprimento desta disposição, sujeitará a responsabilização, podendo incorrer nas penas previstas em lei, conforme sua gravidade e prejuízo ao TJRR.

CAPÍTULO VII
ANÁLISE DE CONFORMIDADE E AUDITORIAS

Art. 28. Ao TJRR é facultada a realização de análises de conformidade ou auditorias periódicas na segurança da infraestrutura de TIC, seus ativos, processos e pessoas com o objetivo de detectar vulnerabilidades e demonstrar evidências do cumprimento da política e boas práticas de Segurança da Informação.

CAPÍTULO VIII
RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 29. É de responsabilidade da STI a implantação de uma equipe de resposta a incidentes de Segurança da Informação, de forma que as fragilidades e eventos de segurança associados aos ativos de informação sejam comunicados a Comissão de Segurança da Informação, permitindo a tomada de ação corretiva em tempo hábil e com a orientação de preservar ou restabelecer operantes os recursos de TIC oferecidos.

Art. 30. A STI tem o dever de guardar as provas produzidas pelos recursos e dispositivos de TIC pelo tempo previsto na tabela de temporalidade do TJRR (DJe Ano XVII – Edição 5208 de 07 de fevereiro de2014), sobretudo em casos de incidente de Segurança de Informação.

CAPÍTULO IX
GERENCIAMENTO DE RISCOS

Art. 31. É de responsabilidade da STI mapear e documentar as ameaças e vulnerabilidades que resultam em risco ao negócio e à infraestrutura de tecnologia que o suporta, assim como buscar a solução adequada para cada caso.

Art. 32. É de responsabilidade da Comissão de Segurança da Informação a administração dos riscos identificados.

CAPÍTULO X
PLANO DE CONTINUIDADE DO NEGÓCIO E RECUPERAÇÃO DE DESASTRES

Art. 33. É de responsabilidade da Comissão de Segurança da Informação coordenar a elaboração, execução, teste e renovação do Plano de Continuidade do Negócio (PCN) que tenha como objetivo minimizar o impacto na disponibilidade dos recursos críticos de TIC e, consequentemente, nos processos do TJRR por eles suportados.

Art. 34. É de responsabilidade da Comissão de Segurança da Informação aprovar a estratégia de continuidade do plano e fornecer subsídios para a sua

implementação.

Art. 35. Independentemente da existência de um Plano de Continuidade dos Negócios ou de Plano Recuperação de Desastres (PRD), a STI deve estabelecer normas e procedimentos para salva guarda de dados com a frequência de realização conforme o grau de importância de cada informação, mantendo sempre os backups tão atualizados quanto possível.

CAPÍTULO XI
VIOLAÇÕES DA PSI E SANÇÕES

Art. 36. Todos os usuários devem noticiar às autoridades responsáveis, como também à Ouvidoria, os incidentes de Segurança da Informação que presenciarem ou tomarem conhecimento, ainda que por mera suspeita, para que providências adequadas sejam adotadas no menor tempo possível, minimizando os danos sofridos pelo TJRR, sem prejuízo de comunicação administrativa conforme o caso e urgência, sendo estes apurados pela Comissão de Segurança da Informação (CSI).

Art. 37. Violações da presente PSI, normas e procedimentos correlatos são passíveis de penalidades administrativas, sem prejuízo de ações legais cabíveis.

Art. 38. Todos os documentos da ENSI do TJRR estão disponibilizados em http://www.tjrr.jus.br/seguranca.

Art. 39. Casos omissos ou esclarecimentos da PSI, normas e procedimentos correlatos são de exclusiva responsabilidade da CSI e passíveis de aprovação pela Presidência do TJRR, conforme o caso.

Art. 40. Esta Resolução entra em vigor na data de sua publicação. Revogando-se outras disposições em contrário.

Publique-se, registre-se e cumpra-se.

Des. ALMIRO PADILHA
Presidente

Des.ª TÂNIA VASCONCELOS DIAS
Corregedora-Geral de Justiça

Des. MAURO CAMPELLO
Membro

Des.ª ELAINE BIANCHI

Membro

Des. LEONARDO CUPELLO
Membro

Dr. JEFFERSON FERNANDES DA SILVA
Juiz Convocado

Fonte: Diário da Justiça Eletrônico. Boa Vista, ed. 5694, p. 2, 03. Mar. 2016.
http://diario.tjrr.jus.br/dpj/dpj-20160303.pdf