Publicação no DJE n.116, de 27/6/2025, p-1-190

RESOLUÇÃO N. 350/2025-TJRO

Revoga a Resolução 088/2019-PR

Revoga o Ato n.111/2020

Institui a Política de Segurança da Informação Cibernética (PSIC) do Poder Judiciário do Estado de Rondônia.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DE RONDÔNIA, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente tecnológico controlado e seguro de forma a oferecer todas as informações necessárias aos processos do Poder Judiciário do Estado de Rondônia com integridade, confidencialidade e disponibilidade.

CONSIDERANDO a necessidade de preservar a credibilidade da instituição, a constante preocupação com a qualidade e celeridade na prestação jurisdicional, bem como a necessidade de assegurar o acesso às informações apenas a usuários(as) autorizados(as);

CONSIDERANDO o aumento contínuo de incidentes cibernéticos na rede mundial de computadores e a necessidade de processos de trabalhos voltados para uma gestão eficaz da segurança da informação;

CONSIDERANDO a Resolução n. 370/2021-CNJ, que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução n. 396/2021-CNJ, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria n. 162/2021-CNJ, que aprova os Protocolos e Manuais criados pela Resolução nº 396/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

CONSIDERANDO a Resolução n. 199/2021-TJRO, que aprova a Política de Privacidade e Proteção de Dados Pessoais no âmbito do Poder Judiciário do Estado de Rondônia;

CONSIDERANDO a Resolução n. 306/2023-TJRO, que dispõe sobre o Sistema de Integridade do Poder Judiciário do Estado de Rondônia;

CONSIDERANDO a Resolução n. 309/2023-TJRO, que dispõe sobre o Código de Ética e Conduta do Poder Judiciário do Estado de Rondônia.

CONSIDERANDO o Ato n. 618/2023-TJRO, que institui o Comitê Gestor de Segurança da Informação e Cibernética Multidisciplinar (CGSI) no âmbito do Poder Judiciário do Estado de Rondônia;

CONSIDERANDO o Ato n. 712/2021-TJRO, que institui a Política de Gestão Documental e de Memória no âmbito do Poder Judiciário do Estado de Rondônia;

CONSIDERANDO os Processos n. 0008319-92.2021.8.22.8000 e 0017780-83.2024.8.22.8000;

CONSIDERANDO a decisão do Tribunal Pleno Administrativo em sessão realizada no dia 23 de junho de 2025,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Seção I
Dos Princípios Básicos

Art. 1º Instituir a Política de Segurança da Informação e Cibernética (PSIC) do Poder Judiciário do Estado de Rondônia (PJRO), na forma desta Resolução e de seus anexos, que tem como princípios básicos:

I - preservação da informação criada e veiculada por meio cibernético;

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

V - orientação à gestão de riscos e à gestão da segurança da informação;

VI - prevenção, tratamento e resposta a incidentes cibernéticos;

VII - articulação entre as ações de segurança cibernética e de proteção de dados e ativos de informação.

Art. 2º Para efeitos desta Política, ficam estabelecidas as seguintes definições:

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

II - ativos de TIC: é o conjunto dos ativos de informação, ativos de rede, processos, funcionalidades e recursos de software e serviços de TIC;

III - crise: um evento ou série de eventos danosos que apresentam propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram, e que apresentam implicações que afetam uma proporção considerável da organização, bem como de seus constituintes;

IV - crise cibernética: decorre de incidentes em dispositivos, serviços e redes de computadores, que causem dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;

V - ativo de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação e os locais onde se encontram esses meios;

VI - confidencialidade: princípio que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada;

VII - integridade: princípio que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

VIII - disponibilidade: princípio que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IX - autenticidade: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

X - gestor(a) de ativo de informação: são os titulares das unidades responsáveis pela gestão e operação dos ativos de informação;

XI - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores, levando à perda de um ou mais princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade;

XII - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do meio em que resida ou da forma pela qual seja veiculado;

XIII - plano de continuidade de tecnologia da informação e comunicação: documentação dos procedimentos e informações necessárias para manter os ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo previamente definido, em casos de incidentes;

XIV - plano de recuperação de serviços essenciais: documentação dos procedimentos e informações necessárias para que se operacionalize o retorno das atividades críticas à normalidade;

XV - público-alvo: é o conjunto de usuários(as) internos(as) e externos(as) atendidos(as) pela área de segurança da informação da STIC;

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

XVII - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XVIII - serviços essenciais de TIC: são aqueles serviços de TIC que suportam os sistemas estratégicos definidos em ato específico, com alto impacto no negócio em caso de indisponibilidade;

XIX - unidade gestora de segurança da informação: é a unidade responsável pela gestão e operação da segurança da informação no Tribunal de Justiça do Estado de Rondônia (TJRO);

XX - usuário(a) interno(a): magistrado(a), servidor(a), prestador(a) de serviço terceirizado, estagiário(a) ou qualquer outro(a) colaborador(a) que tenha acesso autorizado às informações produzidas pelo TJRO;

XXI - usuário(a) externo(a): qualquer pessoa física ou jurídica não caracterizada como usuário(a) interno(a);

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

XXIII - segurança cibernética: conjunto de práticas com foco na proteção digital, que protege informação armazenada nos computadores e aparelhos de computação transmitida através das redes de comunicação informatizada.

Seção II

Das Ações e Objetivos da Política

Art. 3º A Política de Segurança da Informação Cibernética é disciplinada pelo conjunto de normativos que tratam as ações:

I - de gestão em segurança da informação;

II - de segurança da informação das infraestruturas críticas;

III - de tratamento das informações com restrições de acesso;

IV - de proteção dos dados pessoais e dos dados pessoais sensíveis, em conformidade com legislação específica;

V - de prevenção, tratamento e resposta a incidentes cibernéticos;

VI - de gestão e operação de equipe de tratamento e resposta a incidentes cibernéticos;

VII - do estabelecimento dos níveis de maturidade em segurança cibernética; e

VIII - do estabelecimento de processo transparente de comunicação e respostas a incidentes entre o poder público e a sociedade.

Parágrafo único. As ações da Política de Segurança da Informação serão de competência do Comitê Gestor de Segurança da Informação e Cibernética Multidisciplinar (CGSI).

Art. 4º A Política de Segurança da Informação Cibernética tem como principais objetivos:

I - estabelecer diretrizes e normas gerais para a efetiva implementação da segurança da informação cibernética;

II - promover a segurança e defesa cibernética das informações;

III - realizar ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação;

IV - realizar prevenção, tratamento e resposta a incidentes cibernéticos;

V - realizar a segurança da informação em infraestruturas críticas;

VI - promover o tratamento cibernético de informações com restrições de acesso; e

VII - subsidiar a promoção das ações necessárias à implementação e à manutenção dos processos de gestão de riscos, gestão de incidentes de segurança da informação cibernética, gestão da continuidade de serviços essenciais e gestão do uso dos recursos de Tecnologia da Informação e Comunicação.

CAPÍTULO II
DAS COMPETÊNCIAS E RESPONSABILIDADES

Seção I
Dos(as) Usuários(as) de TIC

Art. 5º Os ativos de TIC aos quais os(as) usuários(as) internos(as) tiverem acesso deverão ser utilizados exclusivamente para suas atividades funcionais, de forma ética e garantindo a segurança das informações sob sua competência, conforme o Código de Ética e Conduta e as políticas do PJRO.

Parágrafo único. O compromisso de observância às disposições da Política de Segurança da Informação e Comunicação (PSIC) e de seus anexos será formalizado por meio de assinatura do Termo de Ciência e Compromisso, constante no Anexo II:

I - por servidores(as): no ato da posse ou, a qualquer tempo, por solicitação da Administração;

II - por estagiários(as), voluntários(as), temporários(as) e residentes judiciais: no início das funções ou, a qualquer tempo, por solicitação da Administração; ou

III - por contratados(as) responsáveis pela prestação de serviços terceirizados: na execução contratual.

Art. 6º A inobservância dos dispositivos constantes desta Política de Segurança da Informação Cibernética pode acarretar a aplicação das sanções previstas em lei e normas regulamentares, assegurados aos envolvidos o contraditório e ampla defesa.

Seção II

Do Uso e Gestão da Informação

Art. 7º Na definição das regras de negócio e dos processos de trabalho deverão ser respeitadas as regras do PJRO de privacidade de dados, integridade, segurança da informação cibernética, gestão documental, acesso à informação e legislação correlata.

Art. 8º Cabe ao(à) gestor(a) da cada unidade do TJRO:

I - orientar os(as) usuários(as) sob sua subordinação sobre o uso adequado dos ativos de TIC, conforme as regras estabelecidas neste normativo;

II - reportar à Secretaria de Tecnologia da Informação e Comunicação qualquer descumprimento das diretrizes estabelecidas nesta resolução.

Seção III

Da Secretaria de Tecnologia da Informação e Comunicação

Art. 9º Compete à STIC implantar e gerenciar os controles relativos à gestão:

I - dos ativos de infraestrutura de Tecnologia da Informação e Comunicação, principalmente os críticos e estratégicos;

II - da operacionalização da segurança das configurações da rede de comunicação de dados;

III - da segurança física dos ambientes computacionais com o apoio operacional da unidade responsável pela Segurança Patrimonial e Humana para realizar o controle de acesso físico, a fim de impedir ou repelir o acesso físico não autorizado, a ocorrência de danos e interferências nas instalações e informações digitais do órgão;

IV - das operações tecnológicas;

V - das cópias e restauração de dados do PJRO;

Parágrafo único. Compete ainda à STIC implantar e gerenciar controles relativos ao uso dos recursos tecnológicos e aos acessos às informações e serviços em rede do PJRO.

CAPÍTULO III
DOS PROTOCOLOS DE SEGURANÇA CIBERNÉTICA

Seção I
Do Monitoramento dos Ativos de TIC

Art. 10. O monitoramento contínuo dos ativos de TIC será realizado por unidade operacional da STIC, por meio de testes de invasão e análise de vulnerabilidades que serão tratados da seguinte forma:

I - o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética (GPTIR) atuará de forma preventiva e elaborará planos de ação para tratar de vulnerabilidades detectadas.

II - o GPTIR poderá solicitar apoio multidisciplinar indicado pelo CGSI para elaborar o plano de ação.

III - cabe ao CGSI analisar e aprovar os planos de ação, podendo aplicar alterações.

Seção II
Da Identificação de Incidente de Segurança Cibernética

Art. 11. Qualquer pessoa que identifique uma vulnerabilidade ou incidente com potencial risco à segurança cibernética poderá acionar o GPTIR, devendo formalizar protocolo por meio do Sistema Eletrônico de Informações - SEI, com nível de acesso sigiloso ou restrito.

Parágrafo único. O processamento da informação se dará conforme processos de trabalho estabelecidos pelo GPTIR, Secretaria de Tecnologia da Informação e Comunicação e pelo CGSI.

Art. 12. Ao ser acionado, cabe ao GPTIR:

I - receber, filtrar, classificar e responder as solicitações e alertas, analisando os incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

II - receber informações ou cópia de artefato malicioso que foi utilizado no ataque, ou em qualquer atividade desautorizada ou maliciosa para melhoria nas estratégias de detecção, remoção e defesa contra os artefatos maliciosos;

III - registrar os incidentes de segurança cibernética notificados ou detectados para resguardar o histórico da atuação do grupo.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 13. A Política de Segurança da Informação Cibernética deverá ser revisada anualmente ou a critério do CGSI.

§ 1º Compõem esta Resolução as Normas de Segurança da Informação Cibernética-NSIC contidas nos anexos a seguir:

a) Anexo I - Regras de Sigilo e Confidencialidade;

b) Anexo II - Termo de Ciência e Compromisso com a Política de Segurança da Informação;

c) Anexo III - NSIC 01 - Gestão de Identidade e Controle de Acesso aos Recursos de TIC;

d) Anexo IV - NSIC 02 - Controle de Acesso a Internet;

e) Anexo V - NSIC 03 - Rede Wi-Fi;

f) Anexo VI - NSIC 04 - Acesso Remoto e Uso de VPN;

g) Anexo VII - NSIC 05 - Correio Eletrônico Institucional;

h) Anexo VIII - NSIC 06 - Redes Sociais;

i) Anexo IX - NSIC 07 - Dispositivos de Armazenamento;

j) Anexo X - NSIC 08 - Uso de Software;

k) Anexo XI - NSIC 09 - Equipamentos de TIC e Dispositivos Móveis;

l) Anexo XII - NSIC 10 - Backup e Restauração de Dados;

m) Anexo XIII - NSIC 11 - Acesso aos Datacenters;

n) Anexo XIV - NSIC 12 - Segurança em Nuvem;

o) Anexo XV - NSIC 13 - Desenvolvimento e Obtenção de Software;

p) Anexo XVI - NSIC 14 - Gestão de Vulnerabilidades de TIC.

§ 2º O § 1º deste artigo e os anexos desta Resolução poderão ser revisados por meio de Ato do Presidente do TJRO, mediante iniciativa do CGSI.

§ 3º A STIC elaborará diagnóstico para avaliar a conformidade dos serviços e infraestrutura de TIC com esta Política e submeterá plano de ação ao CGSI para implementar todos os itens.

Art. 14. Os casos omissos serão disciplinados pelo CGSI.

Art. 15. Revoga-se a Resolução n. 088/2019-PR, de 10/04/2019 e o Ato n. 1111/2020, de 26/11/2020.

Art. 16. Esta Resolução entra em vigor na data de sua publicação.

Desembargador Raduan Miguel Filho

Presidente do Tribunal de Justiça do Estado de Rondônia

Documento assinado eletronicamente por **RADUAN MIGUEL FILHO**, **Presidente do Tribunal de Justiça do Estado de Rondônia**, em 26/06/2025, às 13:41 (horário de Rondônia), conforme § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no Portal SEI https://www.tjro.jus.br/sistema-eletronico-de-informacoes-sei, informando o código verificador **4909322** e o código CRC **104D822F**.