ANEXO XVI

RESOLUÇÃO N. 350/2025-TJRO

PODER JUDICIÁRIO DO ESTADO DE RONDÔNIA
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA (PSIC)

NORMA DE SEGURANÇA DA INFORMAÇÃO CIBERNÉTICA

NSIC 14 - GESTÃO DE VULNERABILIDADES DE TIC

PRESIDENTE
Desembargador Raduan Miguel Filho

VICE-PRESIDENTE
Desembargador Glodner Luiz Pauletto

CORREGEDOR-GERAL
Desembargador Gilberto Barbosa Batista dos Santos

SECRETÁRIO GERAL
Juiz Rinaldo Forti Silva

SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO MULTIDISCIPLINAR

Desembargador Glodner Luiz Pauletto

Desembargador Gilberto Barbosa Batista dos Santos

Juíza Valdirene Alves da Fonseca Clementele

Elaine Piacentini Bettanin

Jucélio Scheffmacher de Souza

Ângela Carmen Szymczak de Carvalho

Rosemeire Moreira Ferreira

Fabiano Sergio Paiva Dias de Sá

Gustavo Luiz Sevagnan Nicocelli

Eduardo Luiz Will Bezerra

Reginaldo de Souza Gadelha

Ignácio de Loiola Reis Junior

Hilton José de Santana Pinto

COMITÊ DE GESTÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Ângela Carmen Szymczak de Carvalho

Alessandra Lima Costa

Reginaldo de Souza Gadelha

Simone Soares Sena de Oliveira

EQUIPE DE ELABORAÇÃO

Allan Tito Leite Ratts

Ângela Carmen Szymczak de Carvalho

Fernanda Soares Lana

Ignacio de Loiola Reis Junior

Jorge Willians da Silva Ferreira Batista
Reginaldo de Souza Gadelha
Sidnei Roberto Feliciano da Silva
Simone Soares Sena de Oliveira
Tárik Kamel de Oliveira
Thiago Fleury Marques Cotrim

REGISTRO DE REVISÕES

Política de Segurança da Informação (PSI)				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	novembro/2014	Criação da política.	Sesinf	Coinf
2	janeiro/2017	Acréscimo de critérios para acessar o datacenter principal. Formalizada por meio da Resolução n. 036/2016, republicada em 2017 por erro material.	DISEIN DIESE	Tribunal Pleno
3	abril/2019	Atualização da Política. Formalizada por meio da Resolução n. 088/2019.	DISEIN DIESE	CGSI
4	novembro/2020	Alteração na gestão do serviço de correio eletrônico institucional. Formalizada por meio do Ato n. 1.111/2020.	DESEIN DISEIN DIESE	CGSI
5	junho/2021	Atualização sobre a atuação do Comitê Permanente de Segurança do Poder Judiciário. Formalizada por meio da Resolução n. 209/2021.	DESEIN DISEIN DIESE	CGSI
Política da Segurança da Informação Cibernética (PSIC) **NSIC 14 - Gestão de Vulnerabilidades de TIC**				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos	DESEIN DISEIN DIESE	Cgestic CGSI

		específicos para tratar cada tema individualmente.		

1 OBJETIVO

Estabelecer diretrizes, padrões e boas práticas para a gestão de vulnerabilidades em sistemas de informação no âmbito do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 Disciplinar por meio deste normativo a conscientização, controles e os requisitos mínimos de segurança da informação para a Gestão de Vulnerabilidade de TIC;

2.2 Proteção da Confidencialidade, Integridade, Disponibilidade e Autenticidade das Informações do PJRO;

2.3 Alinhamento com as normas, regulamentações e melhores práticas relacionadas à matéria.

3 FUNDAMENTO LEGAL

3.1 Norma Técnica ABNT NBR ISO/IEC 27001:2022, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da Organização;

3.2 Norma Técnica ABNT NBR ISO/IEC 27002:2022, que fornece diretrizes para práticas de gestão de segurança da informação;

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

3.4 Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018, que estabelece regras para o tratamento de dados pessoais, garantindo a privacidade e a proteção das informações, especialmente relevantes no contexto judiciário;

3.5 Lei de Acesso à Informação (LAI) - Lei nº 12.527/2011, que regulamenta o acesso a informações públicas, reforçando a importância da segurança na gestão e divulgação dessas informações.

4 GLOSSÁRIO

4.1 Agente de Ameaça: Qualquer entidade que pode causar um impacto negativo num sistema. Pode ser tanto um utilizador mal-intencionado querendo comprometer os controles de segurança do sistema, quanto um desvio acidental do sistema ou uma ameaça física como incêndios ou inundações.

4.2 Ameaça: causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização.

4.3 Vulnerabilidade: é qualquer fragilidade dos sistemas computacionais de redes de computadores que permita a exploração maliciosa e acessos indesejáveis ou não autorizados.

4.4 Risco: potencial associado à exploração de vulnerabilidades de um ativo de informação por ameaças, com impacto negativo no negócio da organização.

4.5 Gestão de Vulnerabilidades de TIC: processo de gestão que visa conhecer, monitorar e tratar vulnerabilidades que afetem os ativos de TIC, minimizando o risco de que as mesmas sejam exploradas.

4.6 Ativo de informação: todo dado ou informação gerado, adquirido, utilizado ou custodiado pela PJRO, assim como qualquer equipamento, software ou recurso utilizado para seu processamento ou armazenamento.

4.7 Serviço de TIC: serviço baseado no uso da Tecnologia da Informação, provido a um ou mais clientes para apoiar os processos de negócio da instituição.

4.8 GPTIR: Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética.

4.9 CGSI: Comitê Gestor de Segurança da Informação e Cibernética Multidisciplinar.

5 CONTROLES

5.1 A gestão dos ativos de informação deverá atender os seguintes parâmetros:

5.1.1 Possuir suporte para recebimento de atualizações de segurança.

5.1.2 Receber atualizações de segurança até no máximo 3 (três) meses após a data de liberação oficial da atualização.

5.1.3 Atualizar ativos de alto ou médio risco assim que surgir uma atualização de segurança de criticidade média ou alta.

5.1.4 Utilizar versão que tenha suporte do fabricante ou fornecedor.

5.1.5 Sofrer varreduras e testes periódicos em busca de vulnerabilidades, conforme disponibilidade de licenças da ferramenta de gestão de vulnerabilidades.

5.2 Os ativos de informação serão classificados pelos seguintes níveis de risco:

5.2.1 Ativos de alto risco: expostos à internet, os controladores de domínio, os servidores de banco de dados, os ativos da infraestrutura de rede, os ativos de virtualização, os orquestradores de container, Firewall de Aplicação e firewall de borda, ou outros que venham a ser implementados com esta característica.

5.2.2. Ativos de médio risco: os ativos de informação não classificados como de alto risco e que suportam serviços essenciais para o PJRO, lidam com dados sensíveis ou com dados pessoais cujo acesso não seja público; e

5.2.3 Ativos de baixo risco: os ativos de informação não classificados como de alto ou médio risco.

5.2.4 As atualizações de segurança devem ser aplicadas para, no mínimo, os ativos de informação elencados abaixo:

5.3 As atualizações de segurança devem ser aplicadas, no mínimo, mas não se limitando, para os ativos elencados abaixo:

5.3.1. Os sistemas em uso pelo tribunal, sejam eles adquiridos ou obtidos da comunidade de software livre ou obtidos de outros órgãos Públicos;

5.3.2. As bibliotecas e dependências utilizadas pelos sistemas de informação;

5.3.3. Os servidores de aplicação e os ambientes de execução;

5.3.4. Os Sistemas Gerenciadores de Banco de Dados;

5.3.5. Os Sistemas Operacionais juntamente com pacotes, serviços e programas de máquinas servidoras da rede, físicas ou virtuais;

5.3.6. O firmware dos equipamentos de rede, físicos ou virtuais;

5.3.7. A infraestrutura de virtualização;

5.3.8. Os Sistemas Operacionais e aplicativos das estações de trabalho, físicas ou virtuais;

5.3.9. Os sistemas de “Internet das Coisas” - IOT.

5.4 Os testes e varreduras podem ser realizados de forma automatizada e/ou manual e são classificados em:

5.4.1 Completa: abrange todas as vulnerabilidades conhecidas dos ativos de informação.

5.4.2 Rápida: focadas nas principais vulnerabilidades conhecidas.

5.5 Deve ser executada uma programação mínima de varreduras, conforme detalhado a seguir:

5.5.1 Varredura completa diária nos ativos de informação classificados como de alto ou médio risco, preferencialmente fora do horário de expediente.

5.5.2 Varredura rápida semanal em toda faixa de endereçamentos IP dos ativos de informação do tribunal, preferencialmente fora do horário de expediente.

5.5.3 Varredura por amostragem ou em todas as estações de trabalho, considerando os diferentes tipos de imagem de estação de trabalho.

5.5.4 Varredura por amostragem ou em todas as impressoras, switches, roteadores, equipamentos NAS e dispositivos IOT, considerando os diferentes tipos de dispositivos.

5.5.5 Deverão ser realizadas varreduras e testes conforme frequência e abrangência necessárias, além das previstas na rotina.

5.6 As vulnerabilidades encontradas nas varreduras e testes serão classificadas de acordo com o nível de criticidade, potencial de dano e a facilidade de exploração por ameaça.

5.7 As vulnerabilidades serão classificadas, no mínimo, com os seguintes níveis: crítico, alto, médio, baixo e informação.

5.8 O tratamento das vulnerabilidades encontradas deverá ser priorizado de acordo com o risco do ativo e a criticidade da vulnerabilidade.

5.9 As vulnerabilidades classificadas como críticas ou altas em ativos de alto ou médio risco deverão ser tratadas imediatamente.

5.10 No caso de impossibilidade de tratamento de alguma vulnerabilidade classificada como crítica, o GPTIR deverá ser imediatamente comunicado pela área técnica responsável pelo tratamento.

5.11 A área responsável pelo ativo de informação cujas vulnerabilidades forem encontradas deve atuar para diminuir a exposição ao risco a um nível aceitável, de acordo com o nível de risco do ativo.

5.12 Os processos de correção de vulnerabilidades de criticidade crítica ou alta em ativos de alto ou médio risco, devem ter suas atividades priorizadas em relação às demais atividades rotineiras das unidades técnicas.

5.13 Em caso de ativo de informação que apresente vulnerabilidade, mas não foi desenvolvido ou é mantido pelo PJRO, o órgão deverá ser comunicado para que trate a vulnerabilidade de acordo com seu risco, sob pena de ser retirado da infraestrutura de TIC.

5.14 Deverão ser acompanhados, ao longo do tempo, o surgimento de novas vulnerabilidades, o tempo de tratamento das vulnerabilidades descobertas e o nível de exposição dos principais ativos de informação.

5.15 Cabe à Divisão de Segurança da Informação:

5.15.1 Acompanhar a evolução das vulnerabilidades do ambiente computacional;

5.15.2 Acompanhar a evolução das ameaças de maior prevalência no tocante à segurança de ativos de informação;

5.15.3 Realizar e supervisionar a realização de testes e varreduras nos ativos de informação;

5.15.4 Acionar as áreas técnicas responsáveis pelos ativos de informação, eventualmente vulneráveis, para que providenciem o tratamento;

5.15.5 Elaborar análises de risco de segurança dos ativos de informação, de acordo com as normas de gestão de riscos vigentes;

5.15.6 Reportar-se ao GPTIR sobre a evolução, os riscos e os achados dos testes e varreduras; e

5.15.7 Definir, em conformidade com este normativo, a priorização para a correção das vulnerabilidades encontradas.

5.16 Cabe às unidades técnicas responsáveis pelos ativos de informação:

5.16.1 Apoiar Divisão de Segurança da Informação na configuração dos testes e varreduras de vulnerabilidades;

5.16.2 Acompanhar a realização de testes e varreduras nos ativos de informação;

5.16.3 Providenciar as atualizações de que trata este normativo;

5.16.4 Providenciar a atualização de versão ou migração dos ativos que estão com versão prestes a perder o suporte para recebimento de atualizações de segurança;

5.16.5 Corrigir as vulnerabilidades encontradas em observância à priorização definida pelo Disein;

5.16.6 Implementar medidas para mitigar o risco referente às vulnerabilidades que não puderem ser corrigidas tempestivamente.

5.16.7 Manter atualizado o inventário de ativos de informação.

5.17 Cabe ao GPTIR:

5.17.1 Acompanhar a evolução das vulnerabilidades do ambiente computacional;

5.17.2 Reportar-se ao Comitê Gestor de Segurança da Informação (CGSI) sobre a evolução, os riscos e os achados dos testes e varreduras;

5.17.3 Acionar as áreas técnicas responsáveis pelos ativos de informação, eventualmente vulneráveis, para que providenciem o tratamento;

5.17.4 Informar, quando necessário, as áreas de negócio, o encarregado pela proteção de dados pessoais e GGSI, sobre vulnerabilidade crítica descoberta e que não puder ser tratada em tempo adequado;

5.17.5 Aceitar os riscos que não puderem ser tratados ou encaminhá-los para apreciação do CGSI.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, os logs da análise de vulnerabilidades serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por no mínimo 6 (seis) meses e até 12 (doze) meses.

6.2 Em caso de indícios de descumprimento das diretrizes previstas neste normativo, o Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética poderá de ofício ou por determinação do Comitê Gestor de Segurança da Informação e Cibernética realizar auditoria sobre os fatos.

6.3 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Grupo Gestor Permanente de Tratamento e Resposta a Incidentes de Segurança Cibernética serão encaminhados ao Comitê Gestor de Segurança da Informação, para análise e deliberação.

7 DISPOSIÇÃO FINAL

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos e controles ou quando necessário, mediante iniciativa do CGSI.