ANEXO IX

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 07 - DISPOSITIVOS DE ARMAZENAMENTO

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 07 - Dispositivos de Armazenamento				
Nº	**Data**	**Descrição da Mudança**	**Revisor**	**Aprovador**
1	junho/2025	Alteração na Resolução para focar na segurança da informação cibernética e criação de anexos específicos para tratar cada tema individualmente.	DESEIN DISEIN DIESE	Cgestic CGSI

1 OBJETIVO

Estabelecer diretrizes e padrões para o uso dos dispositivos de armazenamento no âmbito do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 Disciplinar, por meio da conscientização e controles, o uso aceitável dos dispositivos de armazenamento no PJRO;

2.2 Proteger a confidencialidade, integridade, disponibilidade e autenticidade das informações do PJRO;

2.3 Alinhar-se às 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 **Dispositivo institucional de armazenamento:** destinado ao armazenamento local de dados (estação de trabalho, notebook), fornecido pelo PJRO e categorizado como infraestrutura de TIC, que dispõe de controle de acesso e monitoramento.

4.2 **Dispositivo institucional de armazenamento externo:** destinado ao armazenamento de dados (pendrive, HD externo, DVD, etc), fornecido pelo PJRO e categorizado como infraestrutura de TIC, que dispõe de controle de acesso e monitoramento.

4.3 **Dispositivo particular de armazenamento externo**: destinado ao armazenamento de dados (pendrive, hd externo, dvd, etc), não fornecido pelo PJRO, que dispõe de controle de uso e monitoramento.

4.4 **Dispositivo de armazenamento em rede:** destinado ao armazenamento de dados (*storage* em rede, servidores, entre outros), fornecido pelo PJRO e categorizado como infraestrutura de TIC, que dispõe de controle de acesso, monitoramento, controle de capacidade e cópia de segurança (backup).

4.5 **Dispositivo de armazenamento em nuvem:** destinado ao armazenamento de dados em nuvem corporativa, fornecido pelo PJRO e categorizado como infraestrutura de TIC, que dispõe de controle de acesso, monitoramento, controle de capacidade e cópia de segurança (backup).

4.6 **Confidencialidade**: princípio de que a informação esteja indisponível ou não revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada.

4.7 **Integridade**: princípio de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

4.8 **Disponibilidade**: princípio de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade.

4.9 **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.

4.10 ***Storage***: dispositivo usado para o armazenamento dados.

5 CONTROLES

5.1 Os dispositivos de armazenamento institucional deverão seguir as seguintes diretrizes:

5.1.1 Ser destinados somente ao armazenamento de dados estritamente relacionados às atividades institucionais do PJRO ou à função institucional do usuário que o utilizar.

5.1.2 Utilizar de forma comedida e racionalizada, devendo-se evitar o armazenamento de arquivos dispensáveis, sobretudo quando se tratar do armazenamento de dados em rede ou em nuvem.

5.1.3 Estar disponíveis sempre que necessário, bem como deverão possuir capacidade suficiente para armazenar toda a informação a ele destinada.

5.2 Os dispositivos de armazenamento de rede e suas áreas de dados deverão possuir controle que impeça o acesso não autorizado.

5.3 Os arquivos detectados como malware (vírus, trojan, ransomware), serão automaticamente removidos dos dispositivos de armazenamento pelo sistema de proteção anti-malware do PJRO.

5.4 É vedado os seguintes tipos de arquivos nos dispositivos de armazenamento institucional:

5.4.1 Imagens, áudio e vídeo de qualquer formato, cujo conteúdo não tenha relação direta com as atividades institucionais do PJRO;

5.4.1.1 Os arquivos de imagem, áudio e vídeo, quando autorizados, deverão ser criados e armazenados utilizando, dentre outras características técnicas, padrões de codificação, compressão e resolução, adequados às suas necessidades e que resultem em arquivos do menor tamanho possível.

5.4.1.2 Os arquivos tipificados poderão, mediante devida justificativa e autorização formal do STIC, ser excepcionalmente armazenados na rede.

5.4.2 Arquivos de qualquer natureza relacionados a softwares não homologados pela STIC.

5.4.3 softwares executáveis não licenciados ou não homologados pela STIC.

5.4.4 Arquivos em duplicidade.

5.5 Para o armazenamento de dados institucionais, deverão ser utilizados os dispositivos de armazenamento em rede ou os de armazenamento em nuvem do PJRO, destinados à unidade, conforme orientações da área técnica responsável.

5.5.1 Os recursos de armazenamento citados no item 5.7 devem possuir rotinas de backup.

5.5.2 Os armazenamentos internos das estações de trabalho, os dispositivos de armazenamento externo (como pendrives, HDs externos, entre outros) e as pastas individuais em nuvem institucional não possuem rotinas de backup.

5.6 Não é permitido o compartilhamento de uma pasta local de um computador em rede.

5.7 No gerenciamento de armazenamento, cabe a STIC:

5.7.1 O controle, gerenciamento e monitoramento dos dispositivos de armazenamento institucional;

5.7.2 Providenciar a publicação dos padrões de formato e codificação referidos nesta norma;

5.7.3 Realizar a manutenção da estrutura dos dispositivo de armazenamento em rede e os dispositivo de armazenamento em nuvem do PJRO;

5.7.4 Implementar política de backup para os dispositivo de armazenamento em Rede e os dispositivo de armazenamento em Nuvem do PJRO;

5.7.5 Elaborar e divulgar procedimentos técnicos e as melhores práticas relacionados ao uso e gestão dos recursos de armazenamento.

5.7.6 Notificar o usuário para excluir arquivo detectado como malware ou arquivos que não façam parte das atividades funcionais. Caso o usuário não atenda, a STIC deverá excluir o arquivo.

5.8 As unidades do PJRO, as comissões, os comitês, os grupos e os conselhos poderão possuir uma unidade de armazenamento compartilhado na rede ou nuvem à sua disposição, com acesso restrito aos usuários daquela lotação e destinada ao armazenamento de arquivos estritamente relacionados às suas atividades institucionais.

5.9 O recurso compartilhado destinado à unidade organizacional será considerado uma extensão daquela unidade, para fins de correição e auditoria.

5.9.1 O gerenciamento e organização do recurso compartilhado é de inteira responsabilidade do titular da unidade, devendo-se observar os seguintes procedimentos de eliminação:

5.9.1.1 Eliminar arquivos não inerentes às atribuições funcionais da unidade organizacional, arquivos duplicados, desnecessários, obsoletos ou em desuso.

Seção I

Dispositivo de armazenamento em rede

5.10 O diretório de rede vinculado à unidade organizacional terá seu nome formado pela sigla daquela unidade e sua localização na estrutura de diretórios e deverá refletir a posição hierárquica da unidade no âmbito do PJRO.

5.11 O gestor da unidade, presidente ou responsável pela comissão, comitê, grupo ou conselho poderá criar novas estruturas de diretórios (subdiretórios) dentro dos respectivos diretórios.

5.12 Será concedida permissão de acesso ao usuário, conforme sua unidade de lotação e atribuições funcionais.

5.12.1 Nos casos de alteração da lotação do usuário, o titular da unidade deverá imediatamente solicitar a alteração de acesso desse usuário (mudar grupo AD), através de abertura de chamado para a STIC.

5.12.2 A inclusão e/ou alteração de lotação de usuário deverá ser solicitada pelo(a):

5.12.2.1 Chefe imediato da lotação de destino; ou

5.12.2.2 Chefe imediato da lotação originária.

5.12.3 A STIC fará a inclusão e/ou revogação dos direitos de acesso relacionados à lotação originária e/ou atribuição de novos direitos de acordo com a nova lotação;

5.13 As permissões de acesso poderão ser de leitura, de escrita e de modificação, ou uma combinação dessas, de acordo com os critérios solicitados formalmente pelo titular da unidade à STIC.

Seção II

Dispositivo de armazenamento em nuvem

5.14 Cabe a STIC realizar a organização da pasta raiz das unidades (Drive) compartilhadas em nuvem;

5.14.1 O gestor da unidade, presidente ou responsável pela comissão, comitê, grupo ou conselho poderá criar novas estruturas de diretórios (subdiretórios) dentro dos respectivos diretórios de sua unidade.

5.15 Cabe a STIC dar permissão de gerenciamento ao gestor de cada unidade;

5.15.1 Cada gestor da unidade, presidente ou responsável pela comissão, comitê, grupo ou conselho é responsável por gerenciar e controlar o acesso aos dados compartilhados em suas respectivas pastas, garantindo a segurança da informação dentro da unidade.

5.16 As pastas das unidades compartilhadas em nuvem devem possuir recursos avançados de gerenciamento.

Seção III

Dispositivo de armazenamento Externo

5.17 Os dispositivos institucionais de armazenamento externo serão permitidos nas estações de trabalho utilizadas no PJRO para armazenamento temporário de informações relacionadas às atividades institucionais, e o backup dos dispositivo será de responsabilidade do utilizador do dispositivo.

5.18 Os dispositivos particulares de armazenamento externo serão bloqueados nas estações de trabalho utilizadas no PJRO.

5.18 1 Em casos específicos, os dispositivos particulares de armazenamento externo poderão ser liberados para utilização em mquina específica do PJRO, mediante autorização da STIC.

5.19 Cabe a STIC o gerenciamento e controle do acesso desses dispositivos nas estações de trabalho utilizadas no PJRO.

Seção IV

Da Reutilização de Equipamentos/Dispositivos

5.20 Os equipamentos digitais que forem vistoriados pela STIC e estiverem aptos para a reutilização, deverão ter seus respectivos dados e informações excluídas.

5.20.1 Para a formatação segura dos ativos, deverão ser utilizados programas e ferramentas que efetuem a limpeza segura de disco por meio da formatação de baixo nível, eliminando os vestígios de arquivos antigos que permitam sua recuperação.

5.20.2 Quando a formatação não for possível do ponto de vista técnico, deverá ser elaborado um laudo, apontando a causa da impossibilidade de formatação, e preparado o material para a correta destruição. Após o procedimento, deverá ser documentado o procedimento a que o ativo foi submetido (trituração, desmagnetização, incineração ou amassamento), com a assinatura do responsável.

5.20.3 Todo ativo, antes de ser reutilizado, passará pela STIC, que deverá garantir que todos os sistemas necessários estarão instalados e atualizados.

5.20.4 Os computadores deverão estar criptografados, utilizando para isso ferramentas pelas quais a STIC possa gerenciar as chaves criptográficas, devendo possuir também antivírus gerenciável instalado, atualizado e em funcionamento ativo antes da disponibilização para uso do novo colaborador.

Seção V

Da Criptografia em Equipamentos

5.21 Os computadores, tanto laptops quanto desktops, deverão utilizar criptografia e ferramentas pelas quais a STIC possa gerenciar as chaves criptográficas, a fim de garantir a disponibilidade dos ativos na hipótese de esquecimento de senhas ou de realização de auditorias e investigações internas ou externas decorrentes de incidentes de segurança da informação.

5.21.1 Cabe à STIC o gerenciamento das chaves criptográficas.

5.21.2 O CGSI deverá ter acesso à gestão de chaves criptográficas.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, todos os arquivos armazenados nos dispositivos institucionais serão monitorados, e os registros serão mantidos pela Secretaria de Tecnologia da Informação e Comunicação por, no mínimo, 6 (seis) meses e, no máximo, 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.

6.4 A STIC poderá realizar inspeções periódicas e sem aviso prévio nos dispositivos institucionais de armazenamentos para identificação de arquivos que estejam em desacordo com este normativo. Os arquivos poderão ser sumariamente excluídos pela STIC sem prévio aviso aos usuários, sendo a ocorrência informada ao CGSI e ao responsável pelo recurso.

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.