ANEXO XII

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 10 - BACKUP E RESTAURAÇÃO DE DADOS

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 10 - Backup e Restauração de Dados**				
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 *backup* e restauração de dados no âmbito do Poder Judiciário do Estado de Rondônia.

2 MOTIVAÇÃO

2.1 Disciplinar, por meio da conscientização e controles, o *backup* e a restauração de dados.

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

2.3 Alinha-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 **Administrador de backup**: unidade responsável pelo planejamento de soluções de *backup,* definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas.

4.2 **Ativo:** equipamento físico ou virtual, unidade de armazenamento, aplicação ou dados que possuem importância para a continuidade das atividades e serviços da organização.

4.3 **Backup:** conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação.

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

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

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

4.7 **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.

4.8 **Imagem de backup:** arquivo gerado pela solução de backup, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados.

4.9 **Janela de backup:** período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas.

4.10 **Plano de Continuidade do Ativo (PCA)**: plano que define as etapas necessárias para recuperação dos ativos logo após uma interrupção, identificando também os gatilhos para invocação, as pessoas a serem envolvidas, as comunicações, entre outros. Deve estar aderente ao Processo de Gerenciamento de Continuidade dos Serviços Essenciais.

4.11 **Restauração:** processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup.

4.12 **Retenção:** período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração.

4.13 **Rotina de backup:** procedimento utilizado para se realizar um backup com uma frequência e requisitos pré-determinados.

4.14 **Unidade de armazenamento de backup:** unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais, tais como mídias físicas, mídias digitais (*appliance storages*), nuvem (*cloud storages*), entre outros.

5 CONTROLES

5.1 Todos os *backups* devem ser realizados por meio de rotinas de *backup*, com o auxílio de sistemas de agendamento automatizados implementados pelo administrador de *backup*, em janelas de *backup* adequadas ao ativo envolvido.

5.2 As mídias físicas de *backup* possuirão os seguintes controles:

5.2.1 As mídias físicas de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser devidamente identificadas e acondicionadas em local seco, climatizado e seguro (de preferência em cofres corta-fogo) segundo as normas da ABNT.

5.2.2 O tempo de vida e uso das mídias de backup devem ser monitorados e controlados pelo administrador de backup, com o objetivo de excluir mídias que possam apresentar riscos na gravação ou restauração decorrentes do uso prolongado além do prazo recomendado pelo fabricante.

5.2.2.1 Mídias físicas que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

5.3 Deve-se aderir à estratégia 3-2-1 para garantia de proteção dos dados de backup, realizando 3 cópias dos dados, sendo 2 destas em mídias armazenadas em Unidades de armazenamento de backup distintas, dentro de datacenters distintos e 1 mantida em ambiente seguro fora do PJRO.

5.4 Na situação de erro de *backup* e/ou restauração, é necessário que o procedimento seja feito logo no primeiro horário disponível, assim que o administrador de *backup* tenha identificado e solucionado o problema.

5.4.1 Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse *backup*, eles deverão ser autorizados apenas mediante justificativa de necessidade nos termos do Processo de Gerenciamento de *Backu*p.

5.4.2 Testes de restauração de *backup* devem ser executados por seus responsáveis, nos termos dos procedimentos específicos do referido Ativo, de acordo com o Plano de Continuidade do Ativo.

5.4.2.1 Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

5.5 Para formalizar o controle de solicitação de *backups* e restaurações, deverá ser registrado chamado de solicitação destas rotinas em sistema de atendimento do PJRO, o qual deverá ser preenchido pelos responsáveis pelo Ativo em questão, nos termos do Processo de Gerenciamento de Backup.

5.6 Os colaboradores responsáveis descritos nos devidos procedimentos e/ou na planilha de responsabilidade do Ativo poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

5.7 Os arquivos de *backup*, bem como estratégias e políticas devem auxiliar a garantia da temporalidade dos dados conforme descrito no Plano de Continuidade do Ativo ou na Descrição do Sistema.

5.8 A retenção dos arquivos de *backup* não deve ser confundida com a temporalidade dos dados.

5.9 As orientações para os arquivos de *backup* sugeridas são:

5.9.1 Backups Diários (Incrementais):

5.9.1.1 Retenção mínima: 1 mês.

5.9.1.2 Retenção máxima: 3 meses.

5.9.2 Backups Semanais (Completos):

5.9.2.1 Retenção mínima: 3 meses.

5.9.2.2 Retenção máxima: 6 meses.

5.9.3 Backups Mensais (Completos):

5.9.3.1 Retenção mínima: 6 meses.

5.9.3.2 Retenção máxima: 1 ano.

5.9.4 Backups Anuais (Completos):

5.9.4.1 Retenção mínima: 1 ano.

5.9.4.2 Retenção máxima: 5 anos ou conforme exigências regulatórias específicas.

5.9.5 Dados Críticos e de Longo Prazo:

5.9.5.1 Retenção mínima: Conforme requisitos legais ou regulatórios (geralmente 5 a 7 anos).

5.9.5.2 Retenção máxima: Indefinida para dados de importância histórica ou legal.

5.10 É necessária a previsão, em orçamento anual, da renovação e aquisição das mídias em razão de seu desgaste natural e crescimento do volume de dados a ser protegidos, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

5.11 É necessária a previsão, em orçamento anual, da contratação/atualização/aquisição de equipamentos (*Appliances, robôs de fitas*) e Unidades de armazenamento de backup (*Appliance storages, cloud storages*) em razão de seu desgaste natural e/ou crescimento do volume de dados a ser protegidos.

6 MONITORAMENTO E AUDITORIA

6.1 Por motivos de segurança, os logs dos *backups* 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.

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.