Diário Oficial do Estado de Rondônia nº 96
Disponibilização: 20/05/2026
Publicação: 20/05/2026

RONDÔNIA
Governo do Estado

GOVERNO DO ESTADO DE RONDÔNIA

Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC

Estabelece diretrizes, requisitos e procedimentos para a criação, alteração e exclusão de nomes de registro de domínio para sites, sistemas e demais canais digitais no âmbito do Poder Executivo do Estado de Rondônia.

O SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – SETIC, no uso das atribuições que lhe são conferidas pelo art. 114-A, inciso II, da Lei Complementar Estadual nº 965, de 20 de dezembro de 2017, e considerando a importância de estabelecer padrões institucionais para a gestão, governança, segurança e utilização de dados; da transformação digital no âmbito da Administração Pública, com foco em eficiência, transparência e inovação, assim como diante da necessidade de assegurar conformidade com normas de proteção de dados e segurança da informação;

R E S O L V E:

Art. 1º Estabelecer as diretrizes, requisitos e procedimentos para a criação, alteração e exclusão de de nomes de registro de domínio para sites, sistemas e demais canais digitais a serem observadas pelos órgãos e entidades no âmbito do Poder Executivo do Estado de Rondônia, referentes a zona DNS ro.gov.br.

Parágrafo único. Esta Instrução Normativa não se aplica para os processos de transferência da autoridade, delegação ou de subdomínios.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 2º. Esta norma aplica-se às seguintes unidades e agentes envolvidos na gestão e utilização de serviços DNS no âmbito institucional:

I – unidades organizacionais responsáveis pela administração da infraestrutura de rede e dos serviços de DNS;

II – unidades responsáveis pela segurança da informação, governança e gestão de tecnologia da informação; e

III – parceiros externos formalmente autorizados a utilizar serviços DNS vinculados ao domínio institucional.

Art. 3º. Para fins desta Instrução Normativa, considera-se:

I – DNS (Domain Name System): sistema responsável pela resolução de nomes de domínio em endereços IP;

II – Zona raiz: nível hierárquico superior de administração de nomes de domínio sob controle institucional da Superintendência Estadual De Tecnologia Da Informação E Comunicação – SETIC;

III – Registro DNS: entrada configurada em servidor DNS que associa um nome a um recurso;

IV – Parceiro: entidade externa formalmente autorizada a operar serviços vinculados à infraestrutura institucional;

V – Gestão de vulnerabilidades: processo contínuo de identificação, avaliação, tratamento e monitoramento de falhas de segurança;

VI – Análise de risco: processo de identificação e avaliação de ameaças e impactos sobre ativos de informação.

CAPÍTULO II

PRINCÍPIOS E DIRETRIZES

Art. 4º. A gestão de registros DNS deverá observar os seguintes princípios:

I - segurança da informação;

II - disponibilidade e integridade dos serviços;

III - rastreabilidade das operações;

IV - responsabilidade e segregação de funções;

V - conformidade com políticas institucionais e normas de mercado.

Art. 5º. Constituem diretrizes obrigatórias:

I - toda solicitação deverá ser formalizada e registrada em sistema oficial;

II - a criação de registros DNS deverá ser precedida de validação técnica e de segurança;

III - os registros deverão evitar a exposição desnecessária de ativos internos;

IV - deverá ser estimulado o uso de mecanismos de proteção, incluindo DNSSEC, sempre que aplicável;

V - deverá ser mantido inventário atualizado de registros DNS.

CAPÍTULO III

REQUISITOS PARA CRIAÇÃO DE REGISTROS DNS

Art. 6º. A criação de registros DNS estará condicionada ao atendimento dos seguintes requisitos mínimos:

I – apresentação de justificativa técnica e de negócio;

II – identificação formal do responsável técnico pelo serviço;

III – documentação detalhada do serviço a ser publicado;

IV – classificação do nível de criticidade do serviço;

V – indicação dos controles de segurança implementados.

Art. 7º. A solicitação deverá ser submetida à análise das áreas competentes, incluindo:

I – validação técnica da infraestrutura;

II – análise de conformidade com padrões institucionais;

III – avaliação de riscos de segurança da informação.

CAPÍTULO IV

GESTÃO DE VULNERABILIDADES E SEGURANÇA

Art. 8º. É obrigatória a implementação de processo formal de gestão de vulnerabilidades

para todos os serviços associados aos registros DNS.

Art. 9º. Os serviços deverão:

I – ser submetidos a varreduras periódicas de vulnerabilidades;

II – adotar medidas corretivas em prazos compatíveis com a criticidade;

III – manter evidências documentadas das ações de mitigação.

Art. 10. Não será autorizada a criação ou manutenção de registros DNS quando:

I – houver vulnerabilidades críticas ou altas não tratadas, conforme definição do Art. 11;

II – forem identificados riscos elevados que comprometam a segurança institucional;

III – não houver comprovação de controles mínimos de segurança.

Art. 11. Para os fins desta Instrução Normativa, a classificação da severidade das vulnerabilidades deverá observar metodologia padronizada de avaliação de riscos, preferencialmente o Common Vulnerability Scoring System (CVSS), ou outro modelo tecnicamente equivalente adotado institucionalmente.

§ 1º A classificação das vulnerabilidades observará os seguintes níveis de severidade:

I – Vulnerabilidade crítica: pontuação CVSS de 9,0 a 10,0;

II – Vulnerabilidade alta: pontuação CVSS de 7,0 a 8,9;

III – Vulnerabilidade média: pontuação CVSS de 4,0 a 6,9;

IV – Vulnerabilidade baixa: pontuação CVSS inferior a 4,0.

§ 2º A adoção de metodologia diversa do CVSS deverá observar critérios técnicos formalmente definidos e compatíveis com as diretrizes institucionais de gestão de riscos e segurança da informação.

§ 3º. Na ausência de ferramenta com mensuração automatizada, caberá à área de segurança da informação classificar a severidade com base em critérios técnicos equivalentes.

Art. 12. A Coordenadoria de Segurança da Informação - COSEGI da SETIC poderá:

I – recomendar ajustes ou bloqueios na publicação;

II – determinar a suspensão preventiva de registros DNS;

III – realizar testes de segurança sobre os serviços expostos.

CAPÍTULO V

PROCEDIMENTOS OPERACIONAIS

Art. 13. O processo de criação de registros DNS deverá obedecer ao seguinte fluxo:

I - formalização da solicitação pelo parceiro ou área demandante por meio de sistema oficial da SETIC;

II - avaliação de segurança da informação e emissão de relatório técnico;

III - análise, pelo parceiro ou área demandante, do relatório emitido, com adoção das medidas corretivas eventualmente necessárias;

IV - criação do registro DNS.

Art. 14. As alterações em registros existentes deverão seguir o mesmo fluxo previsto no artigo anterior.

Art. 15. A exclusão de registros DNS deverá ocorrer:

I – mediante solicitação formal;

II – por identificação de obsolescência;

III – por determinação de segurança ou governança.

CAPÍTULO VI

RESPONSABILIDADES

Art. 16. Compete à Coordenadoria de Infraestrutura e Serviços - COINFRA da SETIC:

I – implementar e gerir os registros DNS;

II – manter controles de auditoria;

III – garantir a disponibilidade do serviço.

Art. 17. Compete à Coordenadoria de Segurança da Informação - COSEGI:

I – realizar análise de risco e vulnerabilidade;

II – emitir parecer técnico de segurança;

III – monitorar a exposição de serviços.

Art. 18. Compete aos parceiros:

I – assegurar a segurança dos serviços publicados;

II – manter atualizadas as informações técnicas;

III – cumprir as diretrizes desta Instrução Normativa;

IV – atender às recomendações de segurança.

CAPÍTULO VII

AUDITORIA E CONFORMIDADE

Art. 19. Os registros DNS e os serviços a eles associados estarão sujeitos às seguintes medidas de controle e verificação:

I – realização de auditorias periódicas;

II – monitoramento contínuo de desempenho, disponibilidade e segurança; e

III – execução de testes de segurança destinados à identificação de vulnerabilidades e à mitigação de riscos.

Art. 20. O descumprimento desta Instrução Normativa poderá implicar:

I – suspensão ou remoção do registro DNS;

II – restrição de acesso ao ambiente;

III – aplicação de medidas administrativas cabíveis.

CAPÍTULO VIII

DO CONTATO PARA COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Art. 21. A unidade demandante ou entidade parceira deverá indicar, no ato da solicitação de criação de registro DNS, contato(s) responsável(is) para comunicação de incidentes de segurança da informação relacionados aos serviços publicados.

§ 1º. O contato indicado deverá conter, no mínimo:

I – nome do responsável técnico ou área responsável;

II – endereço de correio eletrônico institucional válido;

III – canal alternativo de comunicação, quando aplicável.

§ 2º. O contato informado deverá permanecer atualizado durante todo o período de utilização do registro DNS.

§ 3º. A unidade ou parceiro deverá manter disponibilidade para atendimento de comunicações relacionadas a incidentes de segurança, especialmente em situações que possam impactar a infraestrutura institucional.

§ 4º. As unidades e entidades parceiras que já possuam registros DNS ativos na data de publicação desta Instrução Normativa deverão informar os contatos referidos no caput do presente artigo no prazo de até 30 (trinta) dias, contado da sua vigência.

§ 5º. O não atendimento ao disposto no parágrafo quarto poderá ensejar medidas administrativas, incluindo a suspensão do registro DNS até a regularização.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 22. Os casos omissos serão resolvidos pelas áreas de governança de tecnologia da informação e segurança da informação.

Art. 23. Esta Instrução Normativa entra em vigor na data de sua publicação.

Porto Velho, data e hora do sistema.

CEL PM RR DELNER FREIRE
Superintendente da SETIC
Decreto de 04 de abril de 2023

Documento assinado eletronicamente por **DELNER FREIRE**, **Superintendente**, em 20/05/2026, às 11:52, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **72413440** e o código CRC **1B462460**.

Referência: Caso responda esta Instrução Normativa, indicar expressamente o Processo nº 0070.000523/2026-70 SEI nº 72413440