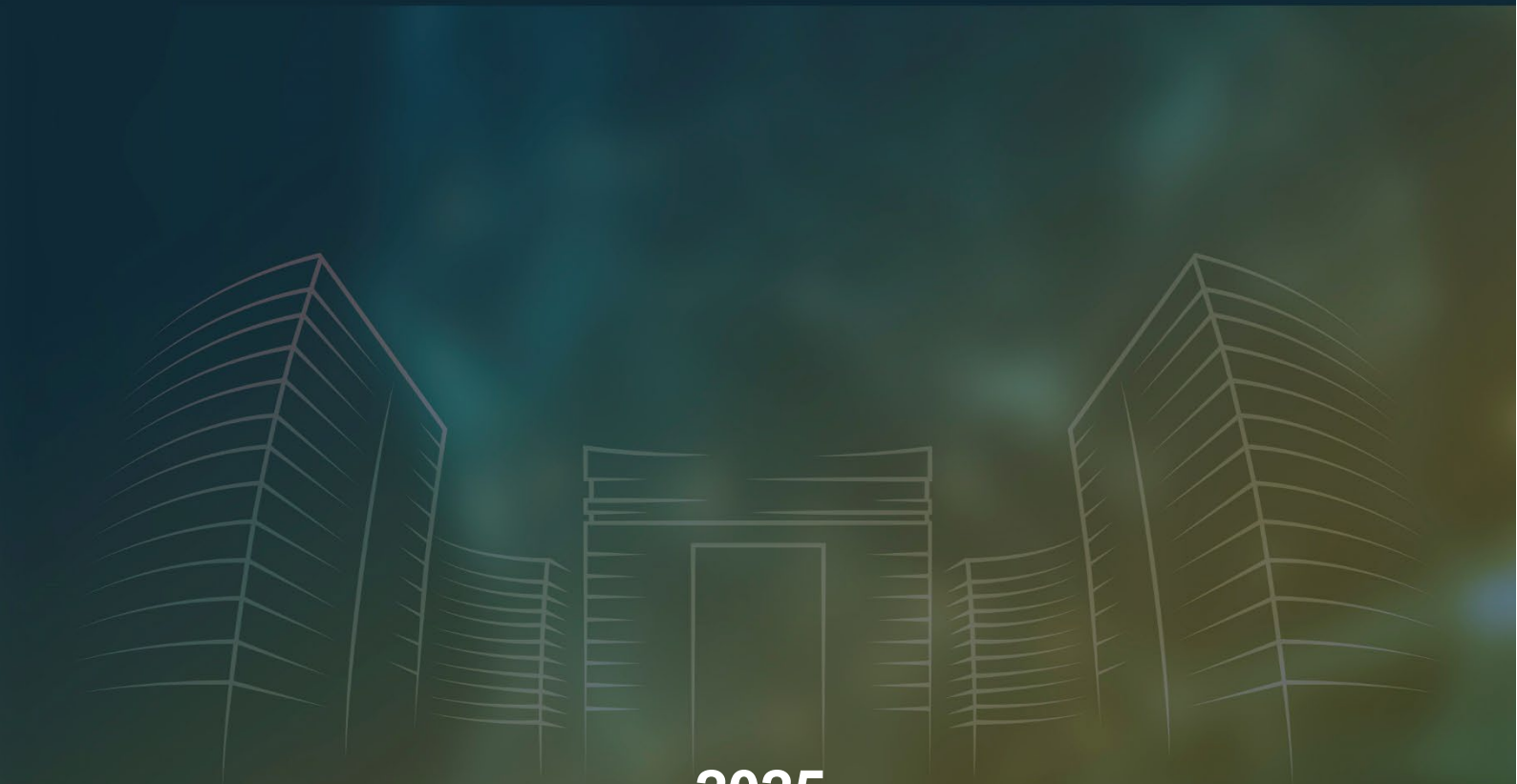
SETIC
Superintendência Estadual de
Tecnologia da Informação
e Comunicação

RONDÔNIA
Governo do Estado

# POLÍTICA DE GESTÃO DE LOG

Portaria nº 134 de 16 de outubro de 2024



2025

**GOVERNO DO ESTADO DE RONDÔNIA**

Marcos José Rocha dos Santos
Governador

Sérgio Gonçalves da Silva
Vice-Governador

**SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO**

Delner Freire
Superintendente

Gabriel Carrijo Bento Teixeira
Diretor Técnico

# SUMÁRIO


**1 INTRODUÇÃO** ..... 2

**2 POLÍTICA DE GESTÃO DE LOG** ..... 3

CAPÍTULO I DISPOSIÇÕES GERAIS ..... 3

CAPÍTULO II DAS REFERÊNCIAS NORMATIVAS ..... 5

CAPÍTULO III DOS REGISTROS DE LOGS ..... 6

CAPÍTULO IV DA CLASSIFICAÇÃO ..... 7

CAPÍTULO V ARMAZENAMENTO ..... 8

CAPÍTULO VI DA PROTEÇÃO DOS REGISTROS DE LOGS ..... 9

CAPÍTULO VII DAS RESPONSABILIDADES ..... 10

CAPÍTULO VIII DO MONITORAMENTO ..... 11

CAPÍTULO IX DOS REGISTROS DE EVENTOS DE USUÁRIOS PRIVILEGIADOS ..... 13

CAPÍTULO X DA SINCRONIZAÇÃO COM O SERVIDOR DE HORÁRIO ..... 14

CAPÍTULO XI DISPOSIÇÕES FINAIS ..... 14

**3 REFERÊNCIAS** ..... 16

# 1 INTRODUÇÃO

Este documento foi fundamentado em diretrizes e normativas que promovem a segurança da informação e a proteção de dados no âmbito da Superintendência Estadual de Tecnologia da Informação e Comunicação (SETIC). Considera-se a Portaria nº 4 de 09 de janeiro de 2023, que institui a Política de Segurança da Informação (PSI), aplicável aos dados e informações trafegadas na rede de dados da SETIC, além de abordar outras providências relevantes.

Reconhecendo a importância de apoiar a gestão de tratamento e resposta a incidentes em redes computacionais, bem como a necessidade de definir processos de gerenciamento e monitoramento de logs em sistemas computacionais, este documento reflete o compromisso em adotar práticas consolidadas e eficazes. As diretrizes aqui apresentadas estão alinhadas às boas práticas descritas nas normas ABNT ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, evidenciando o empenho em assegurar um ambiente computacional seguro e confiável.

Ademais, reforça-se o compromisso com a implementação de controles necessários para o tratamento de dados pessoais, conforme estabelecido pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), reconhecendo que a segurança da informação e a proteção de dados pessoais são condições indispensáveis para a prestação dos serviços institucionais da SETIC. Este documento apresenta, portanto, a Política de Gestão de Log, instituída na Portaria nº 134 de 16 de outubro de 2024, que estabelece uma base para fortalecer as práticas de segurança e promover a excelência operacional.

# 2 POLÍTICA DE GESTÃO DE LOG

**CONSIDERANDO** a Portaria nº 4 de 09 de janeiro de 2023, que Institui a Política de Segurança da Informação - PSI aplicável aos dados e informações trafegadas na rede de dados da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC, e dá outras providências.

**RESOLVE**:

## CAPÍTULO I
## DISPOSIÇÕES GERAIS

**Art. 1º.** Fica instituída a Política de Gestão de Log - PGLog, em conformidade com a Política de Segurança da Informação - PSI da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC.

**Art. 2º.** Este documento estabelece as orientações que devem ser seguidas a fim de garantir a adequada conformidade na administração dos registros de logs destinados à auditoria relacionada à segurança da informação.

**Art. 3º.** Os registros de logs dos ativos tecnológicos devem ser mantidos conforme regulamentam os artigos 5º, 13 e 15 do Marco Civil da Internet (Lei federal nº 12.965/2014).

**Parágrafo único.** Os registros de logs dos ativos tecnológicos devem ser mantidos pelo prazo mínimo de 12 meses, conforme regulamenta o Marco Civil da Internet.

**Art. 4º.** Para os fins do disposto nesta PGLog, abrange:

I - todos os proprietários dos ativos tecnológicos que geram registros de logs para auditoria;

II - todos os colaboradores da SETIC: servidores estatutários ou comissionados, estagiários, menores aprendizes, serviços de terceiros ou indivíduos que direta ou indiretamente, tem a responsabilidade para configurar e manter os registros de logs para auditoria; e

III - todos os processos e procedimentos que assegurem a Gestão de registros de logs de Auditoria, tragam o efetivo retorno e alinhamento com as estratégias da SETIC.

**Art. 5º.** São objetivos desta PGLog:

I - definir diretrizes, procedimentos e responsabilidades para a coleta, armazenamento, uso, retenção e descarte adequados dos registros de logs;

II - assegurar a integridade e a confidencialidade dos registros de logs relacionados à Segurança da Informação;

III - manter uma base disponível, confiável e consolidada de registros de logs para tratamento de incidentes de segurança da informação e auditorias interna e externa;

IV - fornecer diretrizes para a proteção adequada dos registros de logs contra acesso não autorizado, modificação ou exclusão indevida;

V - promover a conformidade com as leis, regulamentos e políticas internas aplicáveis à gestão de registros de logs;

VI - facilitar a rastreabilidade e o monitoramento de atividades relacionadas à Segurança da Informação, permitindo a detecção precoce de incidentes e a tomada de medidas corretivas adequadas;

VII - promover a conscientização e a cultura de segurança entre os colaboradores, destacando a importância dos registros de logs como ferramenta essencial na gestão da Segurança da Informação; e

VIII - estabelecer mecanismos de revisão e melhoria contínua desta PGLog, com base na avaliação de sua eficácia e adequação às necessidades da organização.

**Art. 6º.** Processos, procedimentos e medidas técnicas devem ser definidos e implementados com o objetivo de salvaguardar os dados sensíveis durante todo o seu ciclo de vida.

## CAPÍTULO II
## DAS REFERÊNCIAS NORMATIVAS

**Art. 7º.** A presente PGLog tem como fundamentos as seguintes referências legais e normativas:

I - Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD);

II - Instrução Normativa Estadual nº 1/2022/CGE-CGPD - Política de Privacidade e Proteção de Dados Pessoais Estadual;

III - Lei Federal nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet;

IV - Lei Federal nº 12.527, de 18 de novembro de 2011 - Lei de Acesso à Informação (LAI);

V - Decreto Federal nº 9.637 de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;

VI - Lei Complementar Estadual nº 68, de 09 de dezembro de 1992 - Dispõe sobre o Regime Jurídico dos Servidores Públicos Civil do Estado de Rondônia;

VII - Decreto Estadual nº 9.832 de 12 de junho de 2019 - Dispõe sobre o Comitê Gestor da Segurança da Informação;

VIII - NBR/ISO/IEC 27001/2022 - Estabelece os elementos de um Sistema de Gestão de Segurança da Informação;

IX - NBR/ISO/IEC 27002/2022 - Institui o Código de Melhores Práticas para Gestão de Segurança da Informação;

X - NBR/ISO/IEC 27005:2008 - Diretrizes para o gerenciamento dos riscos de Segurança da Informação;

XI - Cartilha de Segurança para Internet, desenvolvida pelo CERT.br, mantido pelo NIC.br, com inteiro teor em http://cartilha.cert.br/; e

XII - Instruções Normativas do Departamento de Segurança da Informação (DSI) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR): NC 01, 02, 03, 07, 09, 10, 11, 12, 13, 14, 16, 17, 18 e 19.

**Art. 8º.** Para os efeitos desta PGLog, serão utilizados os conceitos e definições do Glossário de Segurança da Informação do Departamento de Segurança da Informação - DSI do Gabinete de Segurança Institucional da Presidência da República - GSI/PR, instituído pela Portaria nº 93, de 26 de setembro de 2019, publicada no Diário Oficial da União em 01/10/2019, edição 190, seção 1, página 3, e disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663 .

## CAPÍTULO III
## DOS REGISTROS DE LOGS

**Art. 9°.** Os registros de logs devem conter informações mínimas e relevantes, com especial atenção para:

I - identificação do usuário que acessou o recurso;

II - identificação dos usuários de origem e destino do evento, quando for o caso;

III - natureza do evento, como sucesso ou falha de autenticação, uso de privilégios, tentativa de troca de senha, criação, modificação ou exclusão de identidades; entre outros;

IV - timestamp, formado por data, hora e fuso horário;

V - endereço de Internet Protocol (IP), portas lógicas, identificador do ativo de processamento, coordenadas geográficas, se disponíveis, e outras informações que permitam identificar a possível origem e destino do evento;

VI - endereços, serviços e protocolos de rede utilizados; e

VII - arquivos acessados e tipo de acesso;

**Art. 10.** Os ativos tecnológicos que não permitam os registros de logs de eventos conforme indicado devem ser mapeados e documentados quanto ao tipo e ao formato de registro de eventos que o sistema permite armazenar.

**Art. 11.** Os registros de logs dos ativos tecnológicos devem ser gerados e retidos de forma adequada para permitir o monitoramento, análise e investigação necessárias.

**Art. 12.** Os ativos tecnológicos classificados com nível de criticidade alta ou crítica, devem ser configurados obrigatoriamente para gerar registros de logs.

## CAPÍTULO IV
## DA CLASSIFICAÇÃO

**Art. 13.** Os ativos tecnológicos em produção devem ser configurados para gerar registros de logs relevantes, conforme sua classificação e armazenados para uso posterior. A classificação dos logs será feita com base nas seguintes características:

I - Propósito:

a. Observabilidade: Explica o porquê de um problema, ajudando a identificar sua causa;
b. Monitoramento: Fornece visibilidade em tempo real sobre o desempenho e integridade do sistema;

c. Auditoria: Garante a rastreabilidade das ações dentro do sistema, útil para segurança e conformidade.

II - Gatilho:

a. Status: Logs que informam mudanças de estado no sistema;
b. Ação: Logs gerados quando ações específicas são realizadas, alterando o estado do sistema.

III - Severidade:

a. Trace/Rastreamento: Nível mais detalhado, para informações granulares;
b. Debug/Depuração: Auxilia na solução de problemas durante o desenvolvimento;
c. Informação: Registra eventos normais do sistema;
d. Alerta/Advertência: Indica situações inesperadas, mas que não afetam diretamente o sistema;
e. Falha/Erro: Registra problemas que afetam parte do sistema;
f. Logs críticos: Indica falhas severas que comprometem a operação do sistema.

IV – Criticidade

a. Baixa: Eventos sem impacto no funcionamento do sistema.
b. Média: Eventos com impacto moderado, exigindo correção, mas sem urgência.
c. Alta: Eventos que afetam a operação e demandam ação rápida.
d. Crítica: Eventos que causam interrupção grave ou total do sistema, exigindo resposta imediata.

## CAPÍTULO V
## ARMAZENAMENTO

**Art. 14.** Os registros de logs devem ser armazenados em um ou mais repositórios centrais.

**Art. 15.** Os registros de logs devem ser armazenados de acordo com as necessidades de retenção de logs, sendo recomendado um período de 6 meses para logs quentes (alta performance) e 12 meses para logs frios (baixa performance).

**Art. 16.** No caso de os registros de logs armazenados conterem informações pessoais, deve-se verificar a conformidade com o Art. 28 da Instrução Normativa Estadual nº 1/2022/CGE-CGPD - Política de Privacidade e Proteção de Dados Pessoais Estadual, para determinar se é necessário eliminar ou manter esses registros após o término do tratamento dos dados pessoais.

**Art. 17.** Os registros de logs devem ser armazenados de acordo com sua criticidade e propósito, observando as seguintes categorias:

I - Logs de Observabilidade: Armazenados em repositórios frios, com retenção recomendada de até 6 meses.

II - Logs de Monitoramento: Armazenados em repositórios de performance intermediária, com retenção de 6 a 12 meses.

III - Logs de Auditoria: Armazenados em repositórios de alta performance, com retenção mínima de 12 meses.

## CAPÍTULO VI
## DA PROTEÇÃO DOS REGISTROS DE LOGS

**Art. 18.** Os arquivos de registros de logs devem ser protegidos para evitar o acesso não autorizado a fim de proteger contra exclusões e mudanças nas informações registradas e/ou a falsificação das mesmas. Com o objetivo de garantir a proteção de que trata o *caput*, os seguintes controles mínimos devem ser implementados:

I - armazenamento em local centralizado e protegido contra acessos indevidos;

II - guarda da cópia centralizada em segmento isolado da rede corporativa, com proteção de dispositivos de segurança, tais como firewall, sistema de detecção e prevenção de intrusões, entre outros;

III - espaço de armazenamento adequado e alertas preventivos de seu esgotamento;

IV - localização física em área com controles de segurança;

V - emprego de protocolos seguros para acesso remoto;

VI - geração de registros de eventos (logs) para todos os trabalhos executados nos arquivos;

VII - conservação de documentação atualizada dos procedimentos de:

a) configuração, instalação e manutenção;
b) administração e operação;
c) cópia de segurança e restauração.

VIII - usuários, incluindo aqueles com direitos de acesso privilegiados, não devem possuir permissão para excluir ou desativar logs de suas próprias atividades.

## CAPÍTULO VII
## DAS RESPONSABILIDADES

**Art. 19.** Os proprietários dos ativos tecnológicos, têm a responsabilidade e autoridade para configurar e manter os registros de logs para auditoria.(Art. 18, Capítulo VII “Das Responsabilidades", PGATIC - SETIC).

**Art. 20.** Em se tratando de infraestrutura ou serviço centralizado, o proprietário pelos serviços ou ativos tecnológicos, tem a responsabilidade de configurar e manter os registros de logs para auditoria.

**Art. 21.** Em se tratando de desenvolvimento de sistemas, o proprietário pelos serviços ou ativos tecnológicos, tem a responsabilidade de configurar e manter os registros de logs para auditoria.

## CAPÍTULO VIII
## DO MONITORAMENTO

**Art. 22.** Os ativos tecnológicos devem ser configurados de forma a gerar registros de logs relevantes, conforme sua classificação e nível de criticidade, com especial atenção para:

I - acesso remoto à rede corporativa;

II - tentativas de autenticação, tanto as bem-sucedidas ou não;

III - criação, alteração e remoção de usuários, perfis e grupos privilegiados;

IV - uso de privilégios;

V - troca de senhas;

VI - modificação de política de senhas, como tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, entre outras;

VII - acesso ou modificação de arquivos, serviços e sistemas de informação considerados críticos;

VIII - acesso ou modificação de documentos e registro de versões;

IX - alteração na configuração de sistemas operacionais, serviços e sistemas de informação;

X - inicialização, suspensão e reinicialização de serviços;

XI - uso de aplicativos e utilitários do sistema operacional;

XII - transações críticas executadas pelos usuários em aplicações e banco de dados tais como acesso a dados sensíveis, operações financeiras, alterações de configurações e permissões, e ações administrativas;

XIII - ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção e prevenção de intrusos;

XIV - acesso físico por senha, cartão magnético ou biometria em área de segurança com ativos tecnológicos críticos como data center, sala de roteadores, entre outros;

XV - acoplamento e desacoplamento de dispositivos de hardware, com especial atenção para mídias removíveis;

XVI - acesso e alteração nos registros de eventos (logs).

**Art. 23.** O monitoramento deve ser executado, de preferência, com o emprego de soluções automatizadas que possibilitem a geração imediata de alertas para eventos críticos, bem como a capacidade de correlacionar e analisar os registros de logs de eventos registrados.

**§ 1º** O monitoramento deve ser executado de modo a preservar a normalidade das atividades no ambiente de produção.

**§ 2º** O nível de monitoramento pode ser diminuído por meio da implementação de controles de acesso que reduzam o risco para os ativos tecnológicos e minimizem a exposição das informações a acessos não autorizados.

**§ 3º** As soluções automatizadas devem passar por análises críticas em intervalos regulares, a fim de ajustar sua configuração e aprimorar a identificação de registros de eventos relevantes, minimizando falsos negativos e falsos positivos.

**§ 4º** Deve-se realizar análises periódicas nos processos de monitoramento, durante a implementação ou manutenção dos ativos

tecnológicos, a fim de assegurar que continuem alinhados com as mudanças que ocorreram.

**§ 5º** Deve ser implementado um espaço de armazenamento adequado e alertas preventivos de seu esgotamento;

**Art. 24.** Os usuários devem estar cientes de que os ativos tecnológicos estão suscetíveis a monitoramento e auditoria sempre que houver suspeita ou constatação de incidente de segurança.

## CAPÍTULO IX
## DOS REGISTROS DE EVENTOS DE USUÁRIOS PRIVILEGIADOS

**Art. 25.** Os registros de eventos dos usuários com privilégios para ações e comandos especiais na rede corporativa, como superusuários, administradores de rede e operadores, entre outros, devem ter mecanismos adicionais de gerenciamento e monitoramento, levando-se em consideração, no mínimo, os seguintes elementos:

I - os registros de eventos dos usuários com privilégios da rede corporativa devem ser protegidos e analisados criticamente, a intervalos regulares;

II - os usuários com privilégios na rede corporativa não devem ter permissão para excluir, modificar ou desativar os registros de eventos relacionados às suas próprias atividades.

## CAPÍTULO X
## DA SINCRONIZAÇÃO COM O SERVIDOR DE HORÁRIO

**Art. 26.** O horário dos ativos tecnológicos deve ser ajustado por meio de mecanismos de sincronização de tempo, garantindo que as configurações de data, hora e fuso horário do relógio interno estejam em sincronia com a Hora Legal Brasileira, de acordo com o serviço fornecido e assegurado pelo Observatório Nacional.

**Art. 27.** A definição correta do horário nos ativos tecnológicos da rede corporativa é importante para assegurar a exatidão dos registros de eventos, que podem ser requeridos para investigações ou como evidências em casos legais ou disciplinares. Deve-se atender, no mínimo, o uso de, pelo menos, 2 (duas) fontes de tempo sincronizadas, a partir das quais os ativos tecnológicos realizem regularmente a recuperação das informações de data, hora e fuso horário, assegurando que os registros de logs sejam consistentes em termos cronológicos.

## CAPÍTULO XI
## DISPOSIÇÕES FINAIS

**Art. 28.** A CPSI decidirá acerca dos casos omissos e das dúvidas surgidas na aplicação desta Política.

**Art. 29.** A não conformidade com esta regulamentação deve ser prontamente registrada como um incidente de segurança e comunicada à CPSI para investigação e implementação das medidas adequadas.

**Art. 30.** Esta política será revisada e atualizada periodicamente, no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata.

**Art. 31**. Esta política será divulgada para todos os que de alguma forma interagem com os ativos tecnológicos da SETIC, garantindo que a conheçam e a pratiquem no desenvolver de suas atividades.

**Art. 32.** Esta Política de Gestão de Log - PGLog entra em vigor na data de sua publicação.

# 3 REFERÊNCIAS

RONDÔNIA. **Portaria nº 4**, de 9 de janeiro de 2023. Institui a Política de Segurança da Informação - PSI aplicável aos dados e informações trafegadas na rede de dados da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC, dá outras providências. Diário Oficial do Governo de Rondônia, Porto Velho, RO, 10 de janeiro de 2023.

RONDÔNIA. **Portaria nº 134**, de 16 de outubro de 2024. Institui a Política de Gestão de Log - PGLog aplicável aos ativos tecnológicos da Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC, e dá outras providências. Diário Oficial do Governo de Rondônia, Porto Velho, RO, 18 de fevereiro de 2025.

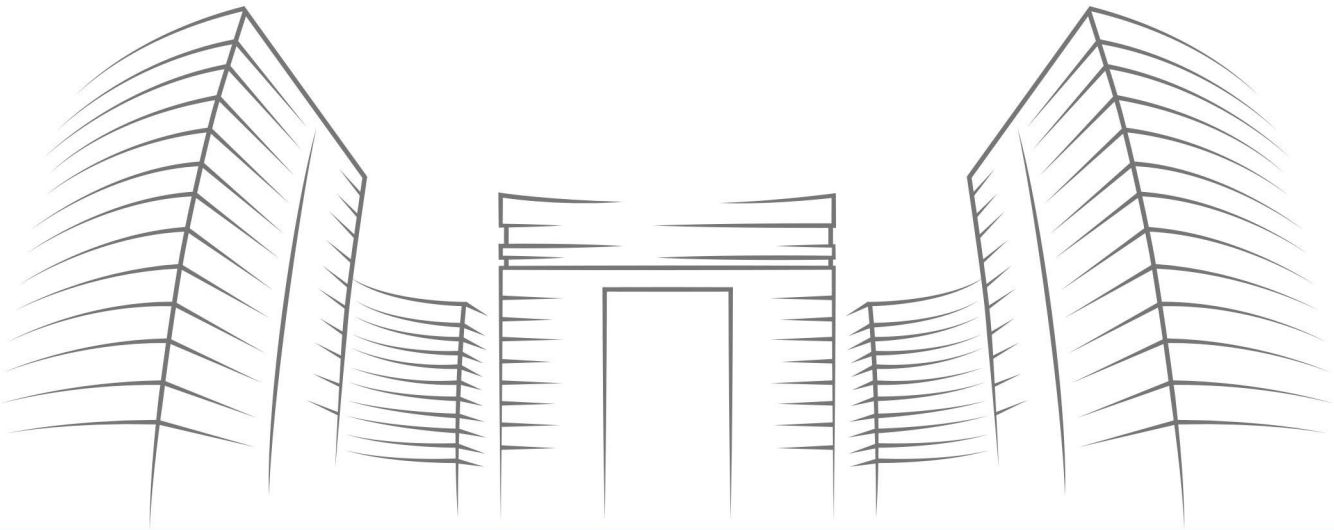
SETIC
Superintendência Estadual de
Tecnologia da Informação
e Comunicação

RONDÔNIA
Governo do Estado

Wiki.SETIC

*Plataforma de Documentação Operacional e Gerencial dos Serviços da SETIC*

wiki.setic.ro.gov.br




setic.ro.gov.br

@setic.rondonia

**Telefone:** 69 3212 9541
**Endereço:** Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470