Diário Oficial do Estado de Rondônia nº 89
Disponibilização: 14/05/2025
Publicação: 14/05/2025

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA

Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC

Instrução Normativa nº 6/2025/SETIC

Dispõe sobre as Diretrizes Gerais de Segurança da Informação no âmbito do Poder Executivo do Estado de Rondônia.

O SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no uso de suas atribuições legais, conferidas pelo Decreto de 01/01/2019, publicado no DOE n. 001, de 03/01/2019, bem como pelo art. 114-A da Lei Complementar Estadual nº 965, de 20 de dezembro de 2017.

R E S O L V E:

Art. 1º Aprovar as Diretrizes Gerais de Segurança da Informação a serem observadas pelos órgãos e entidades no âmbito do Poder Executivo do Estado de Rondônia.

Parágrafo único. Esta Instrução Normativa constituirá as bases para a gestão de segurança da informação, a fim de promover o uso adequado e seguro dos recursos de Tecnologia da Informação e Comunicação - TIC do Poder Executivo Estadual para garantir a continuidade das respectivas atividades e atribuições.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 2º Toda informação gerada ou de qualquer modo processada no âmbito do Poder Executivo do Estado de Rondônia será protegida conforme as diretrizes estabelecidas nesta Instrução Normativa, comprometendo-se os órgãos e entidades deste Poder com a proteção das informações de sua propriedade e/ou sob sua guarda, independentemente do local onde estejam hospedadas.

Parágrafo único. A aplicação das diretrizes desta Instrução Normativa é compromisso das autoridades, servidores, colaboradores, estagiários, prestadores de serviço e de todos aqueles, direta ou indiretamente, envolvidos com os órgãos ou entidades do Poder Executivo Estadual.

Art. 3º Para os fins do disposto nesta Instrução Normativa, a segurança da informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física;

IV - a proteção de dados organizacionais; e

V - as ações destinadas a assegurar a disponibilidade, a integridade e a confidencialidade da informação.

Art. 4º Toda informação gerada, armazenada, processada, transmitida e descartada no âmbito do Poder Executivo do Estado de Rondônia, independente da forma de apresentação ou armazenamento, será considerada patrimônio a ser adequadamente protegido e utilizado exclusivamente para fins relacionados às respectivas atividades institucionais.

§ 1º Os recursos de TIC pertencentes ao Poder Executivo Estadual ou por este disponibilizados para os usuários serão utilizados em atividades estritamente relacionadas às suas funções corporativas.

§ 2º A utilização dos recursos de TIC será monitorada, sendo seus registros administrados e mantidos pelo respectivo setor de TIC de cada órgão ou entidade da Poder Executivo Estadual.

Art. 5º São princípios de segurança da informação, de observância obrigatória independentemente da forma pela qual a informação seja gerada ou manipulada, ainda que por meio físico, virtual ou verbal:

I - confidencialidade, considerando que a informação só deve ser acessível a quem tem a devida autorização;

II - integridade, considerando que a informação deve se manter inalterada desde sua concepção ou alteração autorizada; e

III - disponibilidade, considerando que a informação deve estar sempre disponível às pessoas autorizadas.

Art. 6º A adoção de procedimentos que visem a garantir a segurança da informação deve ser prioridade constante no Poder Executivo Estadual, de forma a reduzir falhas e danos que possam comprometer a imagem do Estado de Rondônia e a continuidade das suas operações ou trazer prejuízos à sociedade.

CAPÍTULO II

DIRETRIZES GERAIS DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 7º No prazo de até 1 (um) ano contado da publicação desta Instrução Normativa, os órgãos e entidades do Poder Executivo Estadual que administrem infraestrutura própria ou sempre que a estrutura, escala e volume das operações de tratamento de dados o exigirem, deverão, de forma gradual, implementar ações de gestão da segurança da informação, observando-se:

I - realizar a análise de riscos voltada à Segurança da Informação;

II - criar e manter uma Política de Segurança da Informação própria, salvo se a Política Estadual de Segurança da Informação já for suficiente, considerando os critérios referidos no *caput* deste artigo e as especificidades do órgão ou entidade;

III - criar e manter um Plano de Continuidade e Recuperação de Serviços;

IV - criar e manter um Plano de Tratamento de Incidentes de Segurança da Informação;

V - constituir uma Equipe de Resposta a Incidentes de Segurança da Informação;

VI - documentar sua infraestrutura de TIC e de procedimentos;

VII - criar e manter uma Política de Geração e Restauração de Cópias de Segurança;

VIII - promover a gestão de Registro de Eventos; e

IX - promover internamente campanhas de capacitação e conscientização em Segurança da Informação.

§ 1º Para os fins desta Instrução Normativa, a análise de riscos voltada à Segurança da Informação é o processo que busca identificar falhas e vulnerabilidades com potencial para expor ou ameaçar dados e informações institucionais, e que faz uso sistemático de informações para identificar fontes de ameaça e estimar riscos.

§ 2 º A análise de riscos voltada à Segurança da Informação é pré-requisito para a execução dos incisos III e IV.

§ 3º A SETIC poderá prestar apoio na criação dos instrumentais previstos no *caput* deste artigo, conforme a sua disponibilidade e a necessidade do órgão ou entidade.

Seção I

Da Política de Segurança da Informação dos Órgãos e Entidades

Art. 8º A Política de Segurança da Informação de um órgão ou entidade é o instrumento formal, aprovado pela autoridade máxima da instituição, dedicado a estabelecer diretrizes locais, responsabilidades, atribuições e outros subsídios para a gestão da segurança da informação no respectivo âmbito interno, obedecidas as normas gerais instituídas pela Política Estadual de Segurança da Informação.

Art. 9º A Política de Segurança da Informação será composta, no mínimo, pelos seguintes itens:

I - escopo, descrevendo o objetivo, abrangência da política e limites dentro dos quais as ações de segurança da informação serão desenvolvidas no órgão ou entidade;

II - conceitos e definições, tendo como base, preferencialmente, o 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, ou sua versão atualizada;

III - princípios que regem a segurança da informação no órgão ou entidade;

IV - diretrizes gerais, abrangendo:

a) controle de acesso;

b) gestão do uso dos recursos operacionais e de comunicações, como dispositivos *endpoint* do usuário, *e-mail*, acesso à internet, mídias sociais, nuvem etc.;

c) segurança na rede local; e

d) trabalho remoto.

V - atribuições, definindo as tarefas e as responsabilidades dos envolvidos na estrutura de gestão de segurança da informação, com orientações mais detalhadas para locais específicos e instalações de tratamento de informações;

VI - penalidades, estabelecendo as consequências para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com o ordenamento jurídico vigente; e

VII - política de atualização, estabelecendo a periodicidade máxima para a revisão da Política de Segurança da Informação e dos respectivos instrumentos normativos, não excedendo a 2 (dois) anos.

Parágrafo único. A Política de Segurança da Informação considerará a natureza e a finalidade do órgão ou entidade e observará o seu planejamento estratégico.

Seção II

Do Plano de Tratamento de Incidentes de Segurança da Informação

Art. 10. O Plano de Tratamento de Incidentes de Segurança da Informação é o instrumento formal que define o processo de tratamento de incidentes de segurança e de privacidade, estipulando etapas e procedimentos bem definidos para evitar incidentes, por meio de identificação prévia, ou nortear as ações de resposta, na hipótese de ocorrência de um incidente, observando:

I - a definição de uma entrada única para relatar eventos de segurança da informação;

II - o estabelecimento de um processo de gestão de incidentes para fornecer à organização a

capacidade de gestão de incidentes de segurança da informação, incluindo administração, documentação, detecção, triagem, priorização, análise, tratamento, comunicação e coordenação de partes interessadas;

III - o estabelecimento de um processo de resposta a incidentes para fornecer à organização a capacidade de avaliar, responder e aprender com os incidentes já tratados; e

IV - a concessão de permissões, apenas para o pessoal competente pré-definido, para lidar com as questões relacionadas a incidentes de segurança da informação dentro da organização.

Art. 11. O Plano de Tratamento de Incidentes de Segurança da Informação deve considerar diferentes cenários hipotéticos, prevendo o desenvolvimento e implementação de procedimentos para as seguintes atividades:

 I - a avaliação de eventos de segurança da informação de acordo com critérios do quê constitui um incidente de segurança da informação;

II - o monitoramento, a detecção, a classificação, a análise e o relatório de eventos e incidentes de segurança da informação, seja por meios dependentes de intervenção humana ou automáticos;

III - a gestão de incidentes de segurança da informação até a sua conclusão, incluindo as fases de resposta e escalonamento, de acordo com o tipo e a categoria do incidente, bem como a possível ativação dos mecanismos de gestão de crises e a ativação de planos de continuidade, a recuperação de incidentes e a comunicação às partes interessadas internas e externas;

IV - o registro de incidentes;

V - o tratamento de evidências digitais; e

VI - a identificação de lições aprendidas e quaisquer melhorias nos procedimentos de gestão de incidentes ou nos controles de segurança da informação em geral que se façam necessários.

Seção III

Da Equipe de Resposta a Incidentes de Segurança da Informação

Art. 12. A Equipe de Resposta a Incidentes de Segurança da Informação é a responsável pela execução dos procedimentos definidos no Plano de Tratamento de Incidentes de Segurança da Informação, por todo órgão ou entidade do Poder Executivo Estadual que possua atribuições relacionadas à administração da infraestrutura de rede de sua organização.

§ 1º A Equipe será instituída por meio do Plano de Tratamento de Incidentes de Segurança da Informação ou por outro ato formal, o qual designará suas atribuições e seu escopo de atuação.

§ 2º A Equipe será composta por servidores públicos previamente designados e com capacitação técnica compatível com suas atribuições.

Seção IV

Da Documentação da Infraestrutura de TIC e de Procedimentos

Art. 13. Os procedimentos de operação dos recursos de tratamento da informação serão documentados e disponibilizados para quem deles necessite, devendo especificar:

I - o inventário e a classificação dos ativos de TIC;

II - as responsabilidades individuais;

III - a instalação e a configuração segura dos sistemas;

IV - a topologia física e lógica da rede local;

V - as instruções para o tratamento de erros ou de outras condições excepcionais;

VI - os contatos de suporte e escalonamento, incluindo contatos de suporte externo em caso de dificuldades operacionais ou técnicas inesperadas;

VII - a gestão das informações de trilha de auditoria e *log* do sistema, bem como o monitoramento de sistemas de vídeo;

VIII - os procedimentos de monitoramento, com destaque para a capacidade, o desempenho e a segurança; e

IX - as instruções de manutenção e garantia dos ativos.

Seção V

Das Campanhas de Capacitação e Conscientização em Segurança da Informação

Art. 14. É dever dos órgãos e entidades do Poder Executivo Estadual promover, periodicamente, a educação, o treinamento e a conscientização sobre o conteúdo da Política Estadual de Segurança da Informação e da Política de Segurança da Informação própria, quando houver, utilizando-se dos meios físicos ou virtuais apropriados.

§ 1º Os órgãos e entidades do Poder Executivo Estadual poderão criar outros programas de educação, treinamento e conscientização sobre segurança da informação, visando assegurar que a organização e as partes interessadas sejam instruídas, sensibilizadas e conscientizadas sobre os potenciais riscos de segurança e de exposição a que estão submetidos os sistemas, as operações e as informações da Administração Pública.

§ 2º Nas ações de educação, treinamento e conscientização, poderão ser aproveitados os conteúdos produzidos pela SETIC ou por outras fontes externas idôneas.

Art. 15. É dever dos órgãos e entidades do Poder Executivo Estadual dar ampla divulgação e participar das campanhas e ações sobre Segurança da Informação promovidas pela SETIC.

Seção VI

Da Política de Geração e Restauração de Cópias de Segurança

Art. 16. Todos os órgãos e entidades que armazenem dados de forma virtual deverão criar uma Política de Geração e Restauração de Cópias de Segurança que atenda aos requisitos de retenção de dados e de segurança da informação.

Art. 17. A Política de Geração e Restauração de Cópias de Segurança discorrerá, no mínimo, sobre os seguintes itens:

I - a produção de registros precisos e completos das cópias de segurança e dos procedimentos de restauração;

II - a definição da extensão e da frequência das cópias de segurança, baseadas nos requisitos de negócios e de segurança da informação da organização;

III - o armazenamento em um local remoto e seguro, a uma distância suficiente para não sofrer danos por qualquer desastre no local principal;

IV - o fornecimento de informações com um nível apropriado de proteção física e ambiental, consistente com as normas aplicadas no local principal;

V - a proteção das cópias de segurança por meio de criptografia, de acordo com os riscos identificados; e

VI - a testagem regular das mídias utilizadas, incluindo seu tempo de vida útil.

Art. 18. As cópias de segurança devem ser mantidas e testadas regularmente e o período de retenção deve considerar as exigências legais pertinentes.

§ 1º Os procedimentos de cópia de segurança para sistemas e serviços individuais serão testados regularmente para assegurar que atendam aos objetivos do Plano de Continuidade e Recuperação de Serviços.

§ 2º Em se tratando de sistemas e serviços críticos, os procedimentos de cópia de segurança devem abranger todas as informações do sistema, aplicações e dados necessários para recuperar o sistema por completo em caso de desastre.

Seção VII

Do Plano de Continuidade e Recuperação de Serviços

Art. 19. O Plano de Continuidade e Recuperação de Serviços é o instrumento formal destinado a identificar e selecionar estratégias de continuidade de TIC, contemplando múltiplas opções de solução para atuação antes, durante e após uma quebra na continuidade dos negócios, e elaborado com base nos resultados da análise de impacto do negócio e no processo de avaliação de risco envolvendo serviços de TIC.

Art. 20. O Plano de Continuidade e Recuperação de Serviços contemplará, no mínimo:

I - as especificações de desempenho e capacidade para atender aos requisitos e objetivos de continuidade de negócios especificados na análise de impacto do negócio;

II - o tempo de recuperação de cada serviço de TIC e os procedimentos para a restauração desses componentes;

III - o ponto de recuperação dos recursos de TIC, definindo informações e procedimentos para a restauração da informação;

IV - controles de segurança da informação, sistemas e ferramentas de suporte; e

V - processos para manter os controles de segurança da informação existentes durante a quebra na continuidade dos negócios.

Seção VIII

Da Gestão de Registro de Eventos

Art. 21. É dever dos órgãos e entidades do Poder Executivo Estadual manter registros auditáveis de atividades, exceções, falhas e outros eventos relevantes gerados pelo sistema operacional e por serviços ou aplicações do dispositivo.

Parágrafo único. Os *logs* e registros dos ativos de informação devem ser criados e retidos em um ou mais repositórios próprios do órgão ou entidade, na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

Art. 22. A geração de registros deve estar habilitada nos ativos de informação, seguindo as diretrizes do processo de gestão de registros de auditoria do órgão ou entidade, devendo ser registrados os eventos de:

a) tentativas de *logon* (do sistema ou domínio) bem-sucedidas e malsucedidas;

b) gerenciamento de contas de usuários;

c) acesso ao serviço de diretório;

d) uso privilegiado;

e) acompanhamento de processos;

f) transações/ações executadas pelos usuários dentro do sistema, bem ou mal sucedidas; e

g) manipulação de *logs*, bem ou mal sucedidas.

Art. 23. Os registros de eventos conterão, no mínimo, os seguintes dados:

a) a identificação do usuário;

b) o tipo de evento;

c) a data e horário;

d) a indicação de sucesso ou falha;

e) a origem do evento; e

f) a identidade ou o nome dos dados afetados, componentes do sistema ou recurso.

§ 1º Ativos de informação que contenham dados sensíveis possuirão *log* de auditoria detalhado.

§ 2º Os registros devem ser mantidos por, no mínimo, o período indicado na legislação vigente.

§ 3º Na hipótese de os registros armazenados conterem dados pessoais, deve-se avaliar se o s *logs* devem ser eliminados ou conservados após o término do tratamento dos dados pessoais, observando o previsto no art. 16 da Lei Geral de Proteção de Dados Pessoais - LGPD.

Art. 24. Deve-se implementar medidas de salvaguarda para os *logs*, bem como controles específicos para o registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto, de forma que estes não tenham permissão para a exclusão ou desativação dos registros (*logs*) de suas próprias atividades.

CAPÍTULO III

DISPOSIÇÕES FINAIS

Art. 25. As novas soluções de tecnologia da informação adquiridas, obtidas por outros meios, desenvolvidas ou implantadas por órgãos e entidades do Poder Executivo Estadual após a entrada em vigor desta Instrução Normativa cumprirão os requisitos de segurança, registro de eventos e auditabilidade nesta dispostos.

Art. 26. Caberá à Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC monitorar a execução das ações estabelecidas nesta Instrução Normativa, podendo solicitar o apoio dos órgãos de Controle Interno.

Art. 27. Esta Instrução Normativa entra em vigor na data de sua publicação.

CEL PM RR DELNER FREIRE
Superintendente da SETIC

Documento assinado eletronicamente por **DELNER FREIRE**, **Superintendente**, em 14/05/2025, às 09:27, 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 **0058653295** e o código CRC **79C6A567**.

Referência: Caso responda esta Instrução Normativa, indicar expressamente o Processo nº 0070.068805/2022-41 SEI nº 0058653295