Diário Oficial do Estado de Rondônia nº 236
Disponibilização: 16/12/2024
Publicação: 16/12/2024

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA

Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC

Instrução Normativa nº 4/2024/SETIC-ASGAB

Dispõe sobre os processos relacionados à gestão de incidentes de segurança da informação nos órgãos e nas entidades da administração pública do Estado de Rondônia.

O SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO, no uso de suas atribuições legais, conferidas pelo art. 114-A da Lei Complementar Estadual nº 965, de 20 de dezembro de 2017, alterado pela Lei Complementar nº 1.062, de 4/6/2020, bem como e;

CONSIDERANDO que compete à SETIC criar e disponibilizar instruções normativas, portarias e regulamentos a respeito das atividades de tecnologia da informação e comunicação, serviços digitais, sites institucionais e portais, bem como fiscalizar e notificar qualquer descumprimento de algum destes dispositivos, conforme art. 114-A, II, da Lei 965/2017;

CONSIDERANDO a necessidade de implementar medidas sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública do Estado de Rondônia

RESOLVE

Art. 1º Aprovar os processos relacionados à gestão de incidentes de segurança da informação nos órgãos e nas entidades da administração pública no Estado de Rondônia.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 2º A presente Instrução Normativa trata dos processos relacionados à gestão de incidentes de segurança da informação que devem ser observados pelos órgãos e pelas entidades da administração pública estadual no planejamento e na implementação de suas ações referentes à segurança da informação.

§ 1º Os conceitos relacionados à temática desta Instrução Normativa estão diretamente ligados a uma série de medidas adotadas estrategicamente para controlar, mitigar e evitar riscos de roubo, danos e perdas dos dados, dispositivos, sistemas e redes, identificando, registrando e combatendo possíveis ameaças.

§ 2º A gestão de incidentes de segurança da informação deve ser mantida e implementada de forma contínua, buscando manter o alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos do órgão ou da entidade.

§ 3º Os processos relacionados à gestão de incidentes de segurança da informação devem estar alinhados com os controles internos de gestão do órgão ou da entidade.

§ 4º Entende-se como incidente de segurança da informação um ou múltiplos eventos de segurança da informação que podem prejudicar os ativos da organização ou comprometer suas operações.

Art. 3º A gestão de incidentes de segurança da informação será constituída pelos seguintes

processos de realização obrigatória pelos órgãos e pelas entidades da administração pública estadual:

I - mapeamento de ativos de informação;

II - análise de riscos de segurança da informação;

III - classificação dos incidentes de segurança da informação;

IV - criação de uma equipe de tratamento e resposta a incidentes;

V - definição de papéis e responsáveis; e

VI - definição de um fluxo de processo de tratamento de incidentes de segurança da informação.

CAPÍTULO II

MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

Art. 4º O processo de mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.

Art. 5º O processo de mapeamento de ativos de informação deve considerar, preliminarmente:

I - os objetivos estratégicos da organização;

II - os processos internos da organização;

III - os requisitos legais; e

IV - a estrutura do órgão ou da entidade.

Art. 6º O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter:

I - os responsáveis - proprietários e custodiantes - de cada ativo de informação;

II - as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação;

III - o método de armazenamento, transporte ou processamento de cada ativo de informação; e

IV - as interfaces de cada ativo de informação e as interdependências entre eles.

Art. 7º O registro de ativos de informação deverá ser homologado por meio de ato do titular do órgão ou da entidade.

Art. 8º Cabe a cada órgão ou entidade designar um agente responsável pela gestão dos ativos de informação, dentre os servidores efetivos do órgão ou da entidade.

Art. 9º Cabe ao agente responsável pela gestão dos ativos de informação:

I - identificar e classificar os ativos de informação por nível de criticidade;

II - identificar potenciais ameaças aos ativos de informação;

III - identificar vulnerabilidades dos ativos de informação;

IV - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório;

V - atualizar periodicamente o relatório mencionado no inciso IV do caput; e

VI - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

CAPÍTULO III

ANÁLISE DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Art. 10. O processo de análise de riscos de segurança da informação tem por objetivo identificar falhas e vulnerabilidades que podem expor dados e informações da organização a ameaças.

Art. 11. O processo de análise de riscos de segurança da informação deve estar alinhado com o modelo de gestão de riscos institucional, compatível com a missão e os objetivos estratégicos do órgão ou entidade, além de considerar, preliminarmente:

I - os processos internos institucionais;

II - os requisitos legais;

III - a política de segurança da informação do órgão ou da entidade;

IV - a política de gestão de riscos institucional, caso exista; e

V - a estrutura do órgão ou da entidade.

Art. 12. O processo de análise de riscos de segurança da informação deverá fornecer à organização o relatório de identificação, análise e avaliação dos riscos de segurança da informação.

Art. 13. A análise de riscos da segurança da informação deve ser regularmente revisada, a fim de manter atualizados os riscos relativos aos ativos de informação.

Art. 14. O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá conter, no mínimo:

I - os riscos associados a cada ativo de informação, considerando as ameaças envolvidas, as vulnerabilidades existentes e as ações de segurança das informações já implementadas;

II - o grau de severidade dos riscos identificados, considerando os valores ou os níveis de probabilidade de ocorrência do risco e as consequências da ocorrência do risco (perda da integridade, disponibilidade, confiabilidade e autenticidade dos ativos envolvidos);

III - os eventos de segurança da informação ocorridos, com a descrição das ações de segurança, e de eventuais consequências do evento para o órgão ou a entidade;

IV - as alterações nos fatores de risco; e

V - as mudanças em relação a critérios de avaliação e análise.

§ 1º O relatório de identificação, análise e avaliação dos riscos de segurança da informação deverá ser atualizado anualmente e sempre que houver alteração em algum dos fatores de risco ou em algum contexto interno ou externo, devendo ser posteriormente enviado ao gestor de segurança da informação para aprovação.

§ 2º Entende-se como contextos interno e externo o conjunto de eventos que possam influenciar a capacidade da organização de atingir seus objetivos estratégicos.

CAPÍTULO IV

CLASSIFICAÇÃO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 15. A implementação do processo de gestão de continuidade de negócios em segurança da informação tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão ou da entidade nessa área, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres.

Art. 16. O processo de gestão de continuidade de negócios em segurança da informação deve ser baseado nas estratégias de continuidade para as atividades críticas, na avaliação dos riscos levantados no processo de gestão de riscos e em diretrizes institucionais sobre gestão de continuidade de negócio.

Art. 17. As diretrizes institucionais sobre o assunto devem ser formalizadas pelo órgão ou pela entidade, contemplando, no mínimo, os seguintes aspectos:

I - consonância com a missão do órgão ou da entidade, considerando sua estrutura, natureza do negócio e sua complexidade, a fim de que a política reflita a cultura e o ambiente institucional;

II - compromissos claros com relação às obrigações legais e regulamentares e à melhoria contínua do processo de gestão de continuidade de negócios em segurança da informação;

III - definição da abrangência e dos limites do processo de gestão de continuidade de negócios em segurança da informação;

IV - identificação de quaisquer autoridades do órgão ou da entidade e delegações necessárias, incluindo os responsáveis por continuidade de negócios na instituição;

V - critérios para o tipo e a escala dos incidentes a serem tratados;

VI - referências às normas, aos regulamentos ou às políticas que convém que o processo considere ou cumpra; e

VII - compromisso de realizar e manter a continuidade do negócio da instituição.

Art. 18. O processo de gestão de continuidade de negócios em segurança da informação deve ser composto por um plano de continuidade de negócios em segurança da informação, o qual observará o disposto no relatório de identificação, análise e avaliação de riscos de segurança da informação e a prioridade de recuperação dos processos de negócio.

Art. 19. O plano de continuidade de negócios em segurança da informação tem por objetivo definir como serão realizadas a gestão dos incidentes em caso de desastres ou de outras interrupções das operações de negócios e a maneira como deverão ser recuperadas as atividades nos prazos estabelecidos.

Art. 20. O plano de continuidade de negócios em segurança da informação deverá conter, no mínimo:

I - o objetivo;

II - as atividades críticas de negócio a serem contempladas no plano;

III - os requisitos para ativação do plano, em especial, o tempo máximo aceitável de permanência da falha;

IV - o(s) responsável(is) pela ativação do plano, com seus respectivos dados de contato;

V - o(s) responsável(is) por aplicar as medidas de contingência definidas, tendo cada servidor responsabilidades formalmente definidas e nominalmente atribuídas, incluindo seus respectivos dados de contato; e

VI - a definição:

a) das ações necessárias para operacionalização das medidas cuja implementação dependa da aquisição de recursos físicos e/ou humanos;

b) dos limites de decisão para os responsáveis pela aplicação das medidas de contingência perante situações inesperadas;

c) dos parâmetros para encerramento do plano e para a volta à normalidade;

d) dos responsáveis por essas ações, incluindo seus dados de contato;

e) da forma de monitoramento desse processo; e

f) de um roteiro de simulação de teste de funcionamento e da forma de sua aplicação.

Parágrafo único. O plano de continuidade de negócios deverá ser testado regularmente, com intuito de que seus resultados sejam documentados e possam garantir a sua efetividade em caso de necessidade de ativação.

Art. 21. A revisão do plano de continuidade de negócios deverá ser realizada:

I - a cada dois anos, no mínimo;

II - em função dos resultados dos testes de funcionamento realizados, uma vez comprovada a perda da validade e eficácia das medidas adotadas diante de novas situações; ou

III - após mudança significativa nos ativos de informação, nas atividades ou em algum de seus componentes.

Art. 22. O gestor de segurança da informação coordenará o processo de gestão de continuidade de negócios em segurança da informação nos seus respectivos órgãos ou entidades, bem como designará um agente responsável pela referida gestão, dentre os servidores efetivos do órgão.

Art. 23. Cabem aos responsáveis pelo processo ou aos titulares das unidades em que forem identificadas atividades críticas as seguintes atribuições:

I - propor as diretrizes a serem contempladas no plano de continuidade de negócios em segurança da informação;

II - elaborar o plano de continuidade de negócios em segurança da informação;

III - realizar os testes de funcionamento desse plano;

IV - avaliar e aprimorar este plano a partir dos resultados dos testes de funcionamento;

V - gerenciar a contingência quando ocorrer a interrupção de atividades, com base nesse plano desenvolvido; e

VI - propor os recursos necessários para a implementação e o desenvolvimento das ações relacionadas à continuidade das atividades, bem como para a realização dos testes de funcionamento deste plano.

Art. 24. Cabe ao agente responsável pela gestão de continuidade de negócios em segurança da informação:

I - assessorar os responsáveis pelo processo ou os titulares das unidades em que forem identificadas atividades críticas nas atribuições descritas no art. 23;

II - avaliar o plano de continuidade de negócios em segurança da informação e propor mudanças, quando aplicável;

III - supervisionar a implementação, os testes de funcionamento e a atualização desse plano;

IV - propor melhorias na implementação de novos controles relativos ao plano de continuidade de negócios em segurança da informação;

V - participar da elaboração da análise de impacto nos negócios; e

VI - propor medidas visando ao desenvolvimento da cultura de gestão de continuidade de negócios em segurança da informação.

CAPÍTULO V

EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES

Art. 25. A Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação é uma equipe que recepciona, analisa, classifica, trata e responde notificações e atividades relacionadas a problemas de segurança da informação.

Art. 26. Deve ser formada por profissionais com experiência técnica de operar os ativos composto do seu inventário a fim de trabalhar com resposta proativa, tratamento passando pelo colegiado quando houver necessidade, se reunindo apenas quando há algum incidente de segurança da informação para ser respondido.

Art. 27. Deve ser reunida apenas quando há algum incidente de segurança da informação para ser respondido.

Art. 28. Em casos de envolvimento de dados pessoais a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação deverá realizar comunicações para o Encarregado de Dados.

CAPÍTULO VI

PAPEIS E RESPONSÁVEIS

Art. 29. Para uma gestão de incidentes de forma efetiva, o órgão deve estabelecer uma equipe de tratamento e os responsáveis chave para a gestão de vulnerabilidades dos incidentes de segurança da informação.

Art. 30. Deve estabelecer o Encarregado pelo tratamento de Dados Pessoais.

Art. 31. Quando necessário e aplicável, poderá estabelecer outros papéis.

Art. 32. Todos os responsáveis e principais atores devem ser elencados e descrito os papéis e responsabilidades pela proteção dos ativos e tratamento dos incidentes de segurança.

CAPÍTULO VII

FLUXO DE PROCESSO

Art. 33. O fluxo do processo servirá para nortear o procedimento de entrada, tratamento e finalização do tratamento de Incidentes de Segurança da Informação.

Art. 34. O fluxo de processo também deverá espelhar a capacidade e especificidade de cada órgão, principalmente referente às etapas do tratamento do incidente, além de disponibilizar as etapas conforme os papeis e responsabilidades.

Art. 35. Ao estabelecer o fluxo de tratamento de incidentes de segurança da informação é importante estabelecer e descrever as etapas do desenho do fluxo.

Art. 36. São consideradas as etapas principais de um fluxo de tratamento de incidentes de segurança da informação:

I - entrada de notificação de incidente, onde será estabelecido um canal único de entrada centralizado para recepção das notificações, detectando a ocorrência ou suspeita de incidente;

II - validação da notificação, onde deve-se coletar as informações sobre o possível incidente, seus riscos de impactos, a criticidade, os danos aparentes e o risco de se agravar, bem como acionar a equipe de tratamento caso tenha algum risco à vida ou segurança de pessoas e informações; e

III - tratamento do incidente, a definição das etapas de tratamento deve ser estabelecida de acordo com o cenário, equipe disponível e conformidade com as legislações vigentes.

§ 1º Os incidentes classificados com nível médio e alto, caso haja necessidade de contenção imediata, devem ser aplicadas medidas emergenciais para a contenção do incidente.

§ 2º Caso o órgão tenha algum colegiado de segurança, confirmado diagnóstico positivo, classificado como grave ou envolvendo dados pessoais, deve ser encaminhado imediatamente para o mesmo.

§ 3º Após a classificação do incidente, sendo o incidente classificados com nível médio ou alto, o órgão deverá comunicar a SETIC para que a mesma reporte a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

Art. 37. Após a aplicação de medidas de contenção imediata, quando necessárias, deverá ser elaborado o Relatório Preliminar, onde deverão ser documentados os dados obtidos durante os estágios iniciais da investigação, a fim de comunicar às partes interessadas a respeito dos próximos passos do tratamento do incidente.

§ 1º Sugere-se que contenham no relatório uma visão geral dos dados disponíveis, uma descrição dos métodos utilizados na coleta de informações, análise preliminar dos resultados e recomendações iniciais.

§ 2º Ressalta-se que um relatório preliminar não é definitivo e pode ser revisado e atualizado à medida que mais informações são obtidas ou análises adicionais são realizadas.

Art. 38. Após o incidente ser contido e tratado deverá ser elaborado um Relatório Final, onde deverão ser documentadas as medidas adotadas para contenção ou erradicação do incidente para futuras proposituras de melhorias de implementações.

Parágrafo Único O relatório final deverá ter a anuência da alta gestão do órgão.

Art. 39. A comunicação das partes interessada é de suma importância e deve estar alinhado ao fluxo dos processos estabelecidos, dessa forma cada órgão deve estabelecer o seu, porém salientamos para observar o meio de comunicação oficial do Governo de Estado, o Encarregado de Dados, o colegiado (caso tenha) e a alta gestão, a fim de tornar mais claro as informações e indivíduos envolvidos.

Art. 40. O Encarregado de Dados deverá, junto ao colegiado (caso tenha) e a alta gestão, quando for necessário, providenciar a comunicação a ANPD e ao titular de dados pessoais sobre a ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares.

Parágrafo Único Quando necessário, o prazo para comunicação de incidente de segurança que afetou dados pessoais à ANPD e ao titular e dados pessoais é de 3 (três) dias úteis, contados do conhecimento pelo controlador.

Art. 41. Ainda quanto os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, deverá ser adotado as providências determinadas pela ANPD tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

Art. 42. Sugere-se a criação de indicadores dos processos para todos os incidentes registrados e acompanhados, contendo o nome do indicador, sua descrição de forma explicativa e a sua métrica.

Art. 43. Após ocorrido um incidente, caso seja necessário a preservação de evidências, deve ser mantido todo o material coletado durante o tratamento do incidente pelo período mínimo de 1 (um) ano.

§ 1º Tal procedimento é prática, antes de se iniciar as ações de restauração de operação do ambiente, a preservação de provas para identificação correta da causa raiz do incidente e, posteriormente, a realização da recuperação dos sistemas afetados.

§ 2º Quando o incidente de segurança da informação envolver dados pessoais, inclusive daquele não comunicado à ANPD e aos titulares, obrigatoriamente deverão ser preservados por 5 (cinco) anos, contados a partir da data do registro, o registro de incidente de segurança assim como as evidências.

CAPÍTULO VIII

DISPOSIÇÕES GERAIS

Art. 44. Os órgãos e as entidades da administração pública estadual devem adotar os processos descritos na presente Instrução Normativa, bem como contemplar em seu planejamento estratégico institucional a gestão de segurança da informação.

Parágrafo único. Para o cumprimento do previsto no caput, os órgãos e as entidades da administração pública estadual devem definir seus próprios planos de ação, com atividades, prazos e responsáveis pela implementação dos processos de gestão de segurança da informação, conforme descrito nesta Instrução Normativa.

Art. 45. Cabe aos órgãos e às entidades da administração pública do Estado de Rondônia:

I - designar, pelo menos, um substituto nos cargos previstos nesta Instrução Normativa, para que possam atuar em caso de impedimentos ou de ausência do titular; e

II - destinar recursos orçamentários para executar as ações de Segurança da Informação previstas nesta Instrução Normativa.

Art. 46. Esta Instrução Normativa entra em vigor na data de sua publicação.

CEL PM RR DELNER FREIRE

Superintendente Estadual de Tecnologia da Informação e Comunicação

Documento assinado eletronicamente por **DELNER FREIRE**, **Superintendente**, em 12/12/2024, às 15:39, 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 **0051099969** e o código CRC **B6AD1D0A**.

Referência: Caso responda esta Instrução Normativa, indicar expressamente o Processo nº 0070.001475/2023-94 SEI nº 0051099969