Diário Oficial do Estado de Rondônia nº 97
Disponibilização: 21/05/2026
Publicação: 21/05/2026

RONDÔNIA
Governo do Estado

GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC

Dispõe sobre a adoção do e-mail institucional como canal oficial para notificações de incidentes cibernéticos, vulnerabilidades e exposições de segurança no âmbito da infraestrutura tecnológica administrada pela Superintendência Estadual de Tecnologia da Informação e Comunicação – SETIC, e dá outras providências.

O SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – SETIC, no uso das atribuições legais que lhe são conferidas pelo art. 114-A, especialmente os incisos I e III, da Lei Complementar nº 965, de 20 de dezembro de 2017,

R E S O L V E:

Art. 1º. Fica instituído o e-mail institucional como canal primário e oficial para o envio de notificações relativas a incidentes cibernéticos, vulnerabilidades e exposições de segurança no âmbito da Administração Pública Estadual e de parceiros que utilizem serviços tecnológicos sob gestão da SETIC.

Parágrafo único. O envio por e-mail institucional poderá substituir ou complementar outros meios de comunicação, sempre que tais meios possam gerar atrasos na adoção de medidas preventivas ou corretivas.

CAPÍTULO I

DAS DEFINIÇÕES

Art. 2º. Para fins desta Instrução Normativa, considera-se:

I – Incidente cibernético: evento adverso que compromete ou tem potencial de comprometer a confidencialidade, integridade ou disponibilidade de ativos de informação;

II – Vulnerabilidade: fragilidade que pode ser explorada para comprometer sistemas, aplicações ou redes;

III – Exposição de segurança: situação em que ativos ou serviços se encontram acessíveis indevidamente ou configurados de forma insegura;

IV – Notificação de segurança: comunicação formal enviada pela SETIC ou por unidade/entidade parceira contendo informações sobre riscos, incidentes ou vulnerabilidades identificadas;

V – Indicadores de comprometimento (IOC): evidências técnicas associadas a atividades maliciosas, tais como endereços IP, domínios, URLs, hashes ou outros artefatos;

VI – Ponto focal de segurança: unidade administrativa ou responsável técnico designado para tratar assuntos relacionados à segurança da informação.

CAPÍTULO II

DA PADRONIZAÇÃO DAS NOTIFICAÇÕES

Art. 3º. As notificações encaminhadas por meio de e-mail institucional deverão conter, sempre que possível, no mínimo:

I – identificação do incidente, vulnerabilidade ou exposição de segurança;

II – descrição sucinta do evento identificado;

III – data e hora da detecção, quando disponível;

IV – identificação dos ativos, sistemas ou serviços afetados;

V – indicadores técnicos disponíveis (IOC);

VI – avaliação preliminar de impacto, quando aplicável;

VII – ações recomendadas ou já adotadas;

VIII – canal de comunicação para retorno e tratativa.

Parágrafo único. A ausência de informações completas não impede o encaminhamento da notificação inicial.

CAPÍTULO III

DO REGISTRO E DA RASTREABILIDADE

Art. 4º. Todas as notificações enviadas e recebidas deverão ser registradas em sistema interno da SETIC, garantindo:

I – rastreabilidade das comunicações;

II – auditoria das ações realizadas;

III – geração de indicadores de segurança;

IV – suporte à análise e melhoria contínua dos processos.

CAPÍTULO IV

DAS JUSTIFICATIVAS E BENEFÍCIOS

Art. 5º. A adoção do e-mail institucional como canal oficial fundamenta-se nos seguintes benefícios:

I – agilidade na resposta: por se tratar de meio de comunicação imediato, possibilita rápida ciência do incidente;

II – direcionamento específico: permite envio direto ao ponto focal de segurança, reduzindo atrasos operacionais;

III – rastreabilidade: possibilita o registro de evidências de envio, recebimento e leitura;

IV – padronização: assegura uniformidade na comunicação de incidentes e vulnerabilidades;

V – redução de burocracia: diminui a necessidade de fluxos administrativos que possam atrasar a mitigação de riscos.

CAPÍTULO V

DAS RESPONSABILIDADES

Art. 6º. Compete à SETIC:

I – monitorar e analisar notificações de segurança recebidas;

II – encaminhar notificações aos responsáveis pelos ativos afetados;

III – manter canais institucionais atualizados;

IV – orientar tecnicamente as unidades e parceiros.

Art. 7º. Compete às unidades administrativas e parceiros:

I – manter atualizado o ponto focal de segurança;

II – monitorar o e-mail institucional informado;

III – comunicar incidentes de forma tempestiva;

IV – adotar medidas corretivas necessárias.

§ 1º. O ponto focal de segurança e os respectivos dados de contato deverão ser permanentemente atualizados, devendo qualquer alteração ser formalmente comunicada à SETIC no prazo improrrogável de 5 (cinco) dias úteis, contados a partir da data da modificação.

§ 2º. A inobservância da atualização cadastral dos contatos poderá inviabilizar a comunicação tempestiva de incidentes, sujeitando a unidade ou parceiro à adoção de medidas administrativas cabíveis por parte da SETIC.

§ 3º. As unidades administrativas e entidades parceiras que já possuam contato cadastrado junto à SETIC deverão validar ou atualizar seus dados no prazo de até 30 (trinta) dias, contado da publicação desta Instrução Normativa.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 8º. A implementação do fluxo de comunicação deverá observar a urgência inerente aos incidentes cibernéticos, priorizando a mitigação de riscos à segurança da informação.

Art. 9º. Os casos omissos serão tratados pela SETIC.

Art. 10. Esta Instrução Normativa entra em vigor na data de sua publicação.

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 14:30, 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 **72463818** e o código CRC **DDEB8B29**.