Diário Oficial do Estado de Rondônia nº 52
Disponibilização: 20/03/2023
Publicação: 20/03/2023

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA

Superintendência Estadual de Tecnologia da Informação e Comunicação - SETIC

INSTRUÇÃO NORMATIVA Nº 01/2023/SETIC/RO

Regulamenta os incisos II e IV do artigo 114-A da Lei Complementar nº 965/2017, definindo testes preventivos pré-definidos de segurança da informação nas modalidades **phishing** e **defacement** simulados.

O SUPERINTENDENTE ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - SETIC, no uso de suas atribuições legais, conferidas pelo artigo 114-A da Lei Complementar Estadual nº 965, de 20 de dezembro de 2017;

CONSIDERANDO que compete à SETIC criar regulamentos a respeito das atividades de tecnologia da informação e comunicação, bem como supervisionar a conformidade das políticas de segurança da informação e comunicação da Administração Pública Estadual, podendo realizar testes preventivos pré-definidos em regulamentações, conforme incisos II e IV do artigo 114-A da Lei Complementar Estadual nº 965, de 20 de dezembro de 2017;

CONSIDERANDO que compete à SETIC estabelecer diretrizes gerais de Política de Segurança da Informação e propor medidas de segurança em tecnologia da informação apropriadas para garantir o atendimento às premissas da LGPD, conforme incisos IV e V, art. 10, Decreto Estadual nº 26.451, de 4 de outubro de 2021;

CONSIDERANDO as atribuições da Coordenadoria de Segurança da Informação - COSEGI da SETIC estabelecidas no regimento interno, Decreto nº 27.577, de 4 de novembro de 2022, artigo 50 e seguintes, envolvendo a prevenção, resposta e tratamento de incidentes de segurança da informação relativos a dados ou ativos tecnológicos afetos à SETIC, bem como a conscientização dos usuários, a fim de manter um nível adequado de conhecimento a respeito de cibersegurança e conformidade legal da tecnologia da informação; e

RESOLVE:

Art. 1º Regulamentar os testes preventivos de segurança da informação voltados à verificação de possíveis vulnerabilidades em ativos tecnológicos do Governo do Estado de Rondônia, nas modalidades **phishing** simulado e **defacement** simulado.

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

I - ativo tecnológico: termo utilizado para fazer referência genérica a itens virtuais e físicos relacionados a Tecnologia da Informação e Comunicação, como sistemas de informação, *softwares*, bancos de dados, sítios eletrônicos, redes, **hardware**, dispositivos de armazenamento, dispositivos móveis e componentes eletrônicos.

II - teste de segurança: ação preventiva controlada e de escopo delimitado, previamente autorizada pela autoridade competente, executada mediante técnicas e procedimentos padronizados com o objetivo de verificar possíveis vulnerabilidades em ativos tecnológicos do Estado de Rondônia, inclusive as decorrentes do comportamento dos usuários, a fim de propor medidas de saneamento.

III - **phishing**: ataque mediante fraude para obter dados pessoais, financeiros e/ou sigilosos de pessoas físicas ou jurídicas, com a utilização combinada de meios técnicos e engenharia social.

IV - **defacement**: ataque a site de internet para obter modificações não-autorizadas de seu conteúdo e/ou estética, com ou sem a utilização de engenharia social.

Art. 3º Compete exclusivamente ao Superintendente da SETIC autorizar a realização de teste de segurança nas modalidades **phishing** simulado e **defacement** simulado.

Parágrafo único. No caso de teste de segurança com potencial para afetar usuários e/ou ativos tecnológicos pertencentes a a outros órgãos ou entidades do Poder Executivo Estadual, a autoridade máxima correlata será cientificada em termos gerais, com, no mínimo, 3 (três) dias de antecedência, cabendo-lhe guardar sigilo sobre o processo para que não prejudique a realização dos testes.

Art. 4º Os testes de segurança de que trata esta Instrução Normativa serão executados exclusivamente pela Coordenadoria de Segurança da Informação - COSEGI da SETIC.

Art. 5º O titular da Coordenadoria de Segurança da Informação - COSEGI poderá propor ao Superintendente da SETIC a realização de teste preventivo, nas modalidades **phishing** simulado e **defacement** simulado, por meio de Plano de Teste de Segurança registrado no Sistema Eletrônico de Informações - SEI, de acesso restrito, que delimitará o escopo do teste, contendo no mínimo:

I - a modalidade do teste a ser realizado;

II - a identificação de nome e matrícula dos servidores da COSEGI autorizados a executar o teste, monitorá-lo e ter acesso aos dados coletados;

III - a finalidade e a justificativa;

IV - a abrangência, identificando quais categorias de usuários e ativos se pretende atingir;

V - o método de atuação, o método de monitoramento e as ferramentas previstas;

VI - a delimitação do período de realização do teste de segurança;

VII - os resultados esperados;

VIII - a forma de tratamento dos dados coletados;

IX - o plano de ação; e

X - o prazo para entrega do relatório dos resultados.

Art. 6º O planejamento e a realização do teste de segurança serão pautados pelas melhores práticas e normas de referência sobre segurança da informação, com destaque para a NBR 27002 e a NBR 27005, podendo abranger a análise de vulnerabilidades, simulação de ataques reais e exploração de falhas com o objetivo de avaliar os riscos associados a potenciais brechas de segurança,

Parágrafo único. O teste de segurança observará os princípios da confidencialidade, integridade e disponibilidade, a não-inserção de dados falsos e a não-modificação, alteração ou exclusão de dados em ativos tecnológicos.

Art. 7º Os dados coletados no decorrer do teste de segurança serão armazenados em servidor de rede localizado no **data center** próprio do Poder Executivo Estadual, mantendo-se os registros de acesso aos mesmos.

§ 1º Fica vedada a coleta de senhas de qualquer natureza.

§ 2º Eventuais dados pessoais ou financeiros coletados durante o teste de segurança serão permanentemente eliminados ou anonimizados no prazo de 3 (três) meses após a emissão do relatório conclusivo.

Art. 8º Concluído o teste de segurança, o titular da COSEGI da SETIC certificará o seu encerramento e apresentará ao Superintendente da SETIC o relatório conclusivo dos resultados obtidos, descrevendo-os em termos qualitativos e quantitativos, e propondo medidas para solucionar ou mitigar as vulnerabilidades detectadas.

§ 1º O relatório conclusivo receberá o grau de acesso restrito e será levado ao conhecimento do Comitê de Privacidade e Segurança da Informação da SETIC e à autoridade máxima do órgão ou entidade responsável pelo ativo tecnológico, cabendo-lhes guardar sigilo do seu inteiro teor.

§ 2º De posse do relatório conclusivo, o órgão ou entidade comunicado na forma do § 1º ficará responsável pela aplicação das medidas para solucionar ou mitigar as vulnerabilidades detectadas, podendo solicitar o apoio técnico da SETIC, no limite das competências desta.

§ 3º O relatório conclusivo não conterá dados pessoais ou financeiros porventura coletados, tampouco identificará as pessoas físicas que se deixaram enganar pelo teste de segurança.

§ 4º As estatísticas e resultados do teste de segurança poderão ser utilizados em campanhas educativas e preventivas de segurança da informação, observado o disposto no §2º deste artigo.

Art. 9º Compete à COSEGI da SETIC monitorar a aplicação das medidas para solução ou mitigação de vulnerabilidades propostas no relatório conclusivo, podendo notificar os responsáveis ou realizar novos testes de segurança, estritamente nos limites do Plano de Teste de Segurança já aprovado e seguindo os mesmos procedimentos.

Art. 10. Constituem faltas funcionais, sem prejuízo da responsabilidade cível e criminal a que se der causa:

I - divulgar, a pessoas não autorizadas, as circunstâncias da execução do teste de segurança ainda não concluído;

II - conceder ou de qualquer modo facilitar o acesso de pessoas não autorizadas aos dados pessoais, financeiros e/ou sigilosos coletados; e

III - agir de modo tendente a frustrar os objetivos do teste de segurança.

Art. 11. Os casos omissos serão resolvidos pelo Superintendente da SETIC.

Art. 12. Esta Instrução Normativa entra em vigor na data de sua publicação.

Porto Velho, 09 de março de 2023.

CEL PM RR DELNER FREIRE

Superintendente da SETIC

Documento assinado eletronicamente por **DELNER FREIRE**, **Superintendente**, em 20/03/2023, às 10:37, 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 **0036415951** e o código CRC **66C9EAE8**.

Referência: Caso responda esta Instrução Normativa, indicar expressamente o Processo nº 0070.000199/2023-47 SEI nº 0036415951