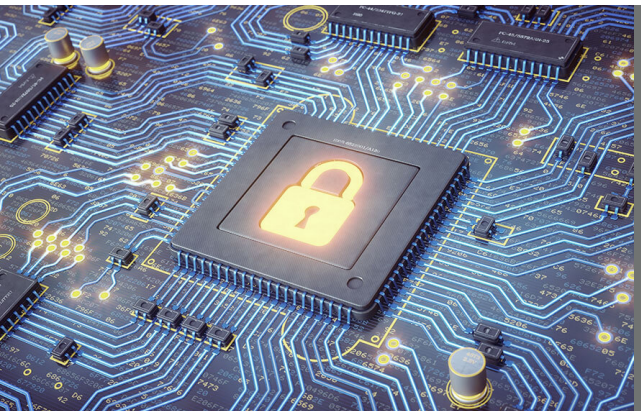

DIREITO DIGITAL E PROTEÇÃO DE DADOS

GUIA DE REFERÊNCIA À PREVENÇÃO E RESPOSTA A RANSOMWARE

21 DE SETEMBRO DE 2026

AUTORES

JULIANA ABRUSIO
SÓCIA / SÃO PAULO

/

/

O Ministério da Gestão e da Inovação em Serviços Públicos (MGI), por meio da Secretaria de Governo Digital (SGD), publicou, recentemente, o **Guia de Referência de Prevenção e Resposta a Ransomware**, elaborado no âmbito do Programa de Privacidade e Segurança da Informação (PPSI 2.0), com execução técnica do CPQD. Trata-se de material voltado especificamente para a modalidade de código malicioso (malware) que utiliza criptografia para sequestrar dados e bloquear sistemas, muitas vezes condicionando o restabelecimento do acesso ao pagamento de resgate.

Embora destinado aos órgãos da Administração Pública Federal, o documento merece atenção também por empresas privadas, pois ele consolida boas práticas de governança, segurança da informação e resposta a incidentes alinhadas a referenciais amplamente reconhecidos, como o NIST CSF 2.0, o CIS Controls e o MITRE ATT&CK. Assim, tende a servir como parâmetro em avaliações de maturidade cibernética e discussões sobre a adequação das medidas de segurança previstas no art. 46 da LGPD.

Além disso, o material reúne orientações relevantes sobre gestão de crises, comunicação de incidentes e preservação de evidências, temas que já possuem impacto regulatório direto para organizações privadas.

A seguir destacamos alguns dos principais pontos do documento.

1. **Ciclo de gestão de incidentes**

O documento organiza a resposta a ransomware em cinco etapas: (1) preparação, (2) detecção e análise, (3) contenção, erradicação e recuperação e (4) atividades pós-incidente.

A abordagem enfatiza a necessidade de integração entre equipes técnicas, jurídico, comunicação, alta administração e encarregado de proteção de dados, reforçando que incidentes cibernéticos devem ser tratados como eventos de negócio, e não apenas questões de TI.

2. **Controles críticos**

O guia estabeleceu uma matriz de priorização com onze controle preventivos fundamentais, funcionando como iniciativas estratégicas de maior impacto para proteção antes de um ataque:

- Estabelecimento de plano formal de resposta a incidentes e gestão de crises;
- Definição de papéis, responsabilidades e fluxos decisórios;
- Programas regulares de treinamento e conscientização;
- Adoção ampla de autenticação multifator (MFA);
- Monitoramento contínuo da infraestrutura;
- Gestão de vulnerabilidades e aplicação de correções de segurança;
- Implementação de backups testados, isolados e protegidos contra alteração;
- Segmentação de rede;
- Controle rigoroso de acessos privilegiados; e
- Mapeamento de sistemas críticos e planejamento de continuidade de negócios.

Embora várias dessas medidas já sejam amplamente adotadas como boas práticas de mercado, o guia tende a reforçar expectativas de contratantes públicos, seguradoras e autoridades sobre o padrão mínimo esperado de diligência em segurança da informação.

3. **Preservação de evidências**

Um dos pontos mais relevantes do documento é a ênfase na preservação adequada de evidências após a identificação de um incidente.

Entre outras medidas, o guia recomenda a preservação de imagens forenses de disco, captura de memória volátil, exportação imediata de logs, preservação das notas de resgate, cálculo de hashes e manutenção de cadeia de custódia.

A recomendação é particularmente importante porque a eliminação prematura de evidências pode comprometer investigações internas, comunicações regulatórias, medidas judiciais e a pretensão indenizatória contra terceiros e o acionamento da apólice.

4. **Seguro cibernético**

O guia chama atenção para um aspecto frequentemente negligenciado durante crises cibernéticas: a observância das condições previstas nas apólices de seguro.

Segundo o documento, é comum que seguradoras exijam: notificação do incidente em curto prazo (muitas vezes entre 24 e 72 horas), utilização de fornecedores previamente aprovados e autorização prévia para determinadas atividades de investigação forense ou resposta.

O descumprimento dessas exigências pode gerar discussões sobre cobertura securitária.

5. **Pagamento de resgate**

O guia orienta o não pagamento com fundamento em normas de direito administrativo, entre elas o princípio da legalidade, a Lei 14.133/2021 e a Lei de Responsabilidade Fiscal.

Embora tais fundamentos não sejam automaticamente extensíveis ao setor privado, a discussão também é relevante para empresas. A avaliação sobre eventual negociação com agentes maliciosos deve considerar aspectos regulatórios, contratuais, reputacionais, securitários e, especialmente, riscos relacionados a sanções internacionais e à identificação da contraparte.

A nossa equipe permanece à disposição para apoiar a revisão de planos de resposta a incidentes, avaliação de apólices de seguro cibernético, adequação de programas de segurança e assessoramento jurídico durante a gestão de incidentes de segurança da informação.