Insuficiente gestión de ciberseguridad en sector público

La CGR emitió un informe de auditoría al **Ministerio de Ciencia Tecnología y Telecomunicaciones** (MICITT) y la **Comisión Nacional de Prevención de Riesgos y Atención de Emergencias** (CNE), respecto de la **gobernanza de la ciberseguridad del país** y si esta responde al marco normativo y prácticas aplicables. Los hallazgos revelan que **el sector público se enfrenta ante la incertidumbre** de no tener claridad sobre la magnitud y cantidad de incidentes que actualmente han logrado vulnerar los sistemas informáticos, con el **potencial de afectar la continuidad de los servicios públicos y la salvaguarda de la información**. A continuación mayor detalle:

Áreas de mejora en gobernanza de ciberseguridad

Principales hallazgos

Carencia de coordinación interinstitucional en un estado de necesidad y urgencia en ciberataques.

Participación intermitente CNE, pese a su rol de liderazgo ante la emergencia. (Decreto Ejecutivo n.° 43542-MP-MICITT)

Gestión inoportuna por parte de Centro de Respuesta de Incidentes de Seguridad Informática (CSIRT-CR) - MICITT. La **CGR encontró 7 entidades públicas con incidentes** materializados, mientras CSIRT-CR solo detectó uno.

Las **alertas técnicas** efectuadas por el MICITT **corresponden a posibles vulnerabilidades** de los sistemas informáticos, **no** así **a ciberataques materializados.**

Inexistente certeza sobre continuidad en gestión de ciberseguridad y adquisición de licencias informáticas para proteger al sector público en su actividad ordinaria.

Informe completo en el enlace a continuación: https://cgrfiles.cgr.go.cr/publico/docs_cgr/2022/SIGYD_D/SIGYD_D_2022026167.pdf
Video de Lía Barrantes, gerente a.i., del área de Fiscalización para el Desarrollo Sostenible: https://www.youtube.com/watch?v=qtK4goBV7Nw