Inacción pone en riesgo seguridad de la información de AyA

La CGR realizó un informe de auditoría en el **Instituto Costarricense de Acueductos y Alcantarillados** (AyA) sobre la **seguridad de la información de los sistemas sustantivos**. El AyA tiene a cargo los servicios públicos de abastecimiento de agua potable y saneamiento de aguas residuales para gran parte de la población y, en la prestación de sus servicios, requiere una infraestructura tecnológica que **soporte y garantice la seguridad de la información en los sistemas más críticos,** dado el alto volumen de información que procesan y la relevancia para el país.

Conviene destacar lo indicado en el informe: *"Lo evidenciado obedece al escaso direccionamiento y monitoreo del jerarca y titulares subordinados para conciliar la seguridad de la información como parte esencial del giro de negocio y la falta de seguimiento en la implementación de las políticas y controles de seguridad de la información... Las situaciones encontradas exponen a la institución a un riesgo de pérdida de confidencialidad, disponibilidad e integridad de la información que se almacena en sus sistemas de misión crítica, así como a una posible interrupción de servicios y tiempo excesivo de recuperación ante un evento..." (*página 4 del informe - resumen ejecutivo).

Hallazgos de la auditoría

 AyA presenta muy **bajo cumplimiento del marco normativo** y buenas prácticas aplicables en materia de seguridad de la información.

 Tiene **débiles controles en materia de ciberseguridad**: sistemas críticos en el AyA presentan vulnerabilidades en cuanto a componentes externos y configuraciones del sitio web.

 **Carencias más relevantes:**

1. Cláusulas de confidencialidad de información y garantía de continuidad del servicio en documentos contractuales para servicios TI.
2. Gestión de cuentas de usuario pese a que el acceso a sistemas está restringido y existe una política de contraseñas.
3. Estrategia de gestión de continuidad del negocio que asegure la provisión de servicios ante eventos que afecten la disponibilidad.
4. Análisis de Impacto del Negocio, ni plan para la Contingencia Tecnológica, sumado a que la programación de respaldos no contempla las pruebas que garanticen su efectividad.
5. Doble autenticación o superior configuración, en controles de autenticación de usuarios y de entrada de datos para los sistemas críticos

Conozca el informe completo en el siguiente enlace: DFOE SOS IAD 00006-2023
Video de Carolina Retana, gerente de Fiscalización para el Desarrollo Sostenible: en este enlace