Gac Sanit. 2026;40(S4):457

Gaceta Sanitaria

https://www.gacetasanitaria.org

385 - VULNERABILIDADES DE DISEÑO EN APLICACIONES DE SALUD PÚBLICA Y SU IMPACTO EN LA PROTECCIÓN DE DATOS

C. Moreno Jódar, J. Juaneda, R. Núñez-Lagos Pérez, P. Hernández López, A. del Cerro Vergara, E.V. Martínez Sánchez, F. Simón Soria

Centro de Coordinación de Alertas y Emergencias Sanitarias, Ministerio de Sanidad; TRAGSA.

Resumen

Antecedentes/Objetivos: La digitalización de la salud pública ha incrementado el uso de aplicaciones informáticas para la gestión de datos poblacionales destinados a la vigilancia. Aunque estos sistemas suelen someterse a controles técnicos y normativos, persisten riesgos derivados de decisiones de diseño que pueden comprometer la confidencialidad, integridad y uso adecuado de los datos personales. El objetivo de este trabajo es describir vulnerabilidades de diseño en aplicaciones de salud pública y analizar su impacto potencial en la seguridad y protección de los datos personales, desde una perspectiva alineada con los principios de protección de datos por diseño y por defecto.

Métodos: Se realizó un análisis técnicófuncional durante las fases finales de validación de diversas aplicaciones de salud pública, previo a su puesta en producción. El análisis se centró en la observación del comportamiento funcional de las aplicaciones desde el punto de vista del usuario, prestando atención a los controles de acceso, la gestión de perfiles profesionales y el tratamiento de datos personales. Los hallazgos se estructuraron mediante un análisis sistemático de riesgos, tomando como referencia marcos de buenas prácticas en ciberseguridad y evaluando su impacto en la confidencialidad, el acceso indebido a información y el cumplimiento del Reglamento General de Protección de Datos.

Resultados: Entre los principales hallazgos se identificaron: Controles de acceso inconsistentes, que permitían a determinados perfiles acceder a información o funcionalidades no acordes con su rol profesional. Deficiencias en la separación de responsabilidades entre el sistema y el usuario, delegando decisiones críticas en mecanismos poco fiables. Desajustes entre la definición funcional de los perfiles profesionales y su implementación, generando accesos no previstos a datos sensibles. Exposición innecesaria de datos personales o metadatos, aumentando el riesgo de identificación indirecta o uso secundario no previsto.

Conclusiones/Recomendaciones: Las vulnerabilidades detectadas no responden a fallos puntuales, sino a decisiones de diseño que limitan la aplicación efectiva de los principios de seguridad y protección de datos desde el inicio. Estos problemas pueden afectar a la confidencialidad de la información, la confianza de la ciudadanía y la calidad de los sistemas de salud pública. Se recomienda integrar la seguridad de la información y la protección de datos como elementos estructurales del diseño de las aplicaciones, con participación temprana de perfiles técnicos, legales y de salud pública.