# FACTORES CLAVE EN LA MADUREZ DE LA SEGURIDAD DE LA INFORMACIÓN: ESTUDIOS EXPERIMENTALES EN EL SECTOR PÚBLICO

**Palabras clave:** diseño experimental, seguridad de la información, nivel de madurez, organización pública.

## Abstract

Se identifican los factores que influyen en el nivel de madurez en seguridad de la información en una organización pública, utilizando un enfoque cuantitativo basado en el Diseño de Experimentos. Se aplicó la encuesta DDISI a 470 funcionarios, evaluando diez dimensiones críticas, lo que permitió recolectar más de 26,000 respuestas y estructurar tres diseños experimentales en R Studio. Los resultados evidencian que el área funcional influye significativamente en la madurez, destacando las áreas de Notificaciones y Desarrollos Tecnológicos con los niveles más altos. Asimismo, el conocimiento sobre temas específicos, como redes sociales y prácticas financieras, se asocia con mayor madurez, mientras que otros, como amenazas latentes y dispositivos domóticos, presentan debilidades. El tipo de vinculación no fue significativo, pero sí el género, con un leve mejor desempeño en hombres. Se concluye que el diseño experimental es eficaz para orientar estrategias de fortalecimiento en seguridad de la información pública.

## Introducción

La seguridad de la información en las instituciones públicas es vital para proteger datos sensibles y garantizar la seguridad nacional (Jevtić & Alhudaidi, 2023; Samara, 2023). Esto incluye la integridad, confidencialidad y disponibilidad de los datos, abordando ciberamenazas complejas (Jevtić & Alhudaidi, 2023). Las instituciones públicas deben priorizar la seguridad de la información y demostrar una mejora continua mediante modelos de madurez de seguridad (Hochstetter-Diez et al., 2023). En este contexto, la creciente digitalización de los procesos administrativos y la exposición a riesgos asociados a factores humanos y vulnerabilidades tecnológicas exigen el fortalecimiento de capacidades organizacionales orientadas a una madurez estructurada en materia de seguridad de la información. Esta investigación tiene como objetivo principal identificar los factores clave que inciden significativamente en el nivel de madurez en seguridad de la información en un organismo público, mediante la aplicación de un enfoque cuantitativo sustentado en el Diseño de Experimentos.

## Metodología

La metodología empleada se estructuró a partir de la aplicación de un instrumento propio desarrollado denominado Diagnóstico de Defensa Digital Individual en Seguridad de la Información (DDISI), diseñado para evaluar diez dimensiones críticas del conocimiento y las prácticas en torno a la seguridad de la información: aplicaciones de mensajería, autenticación, buenas prácticas financieras, correo electrónico, dispositivos domóticos, dispositivos móviles,

equipos de cómputo, navegación web, otras amenazas latentes y redes sociales. La encuesta fue aplicada a 470 funcionarios públicos, lo que permitió recopilar un total de 26,000 respuestas, generando una base de datos estadísticamente robusta, con la cual se plantearon 3 diseños experimentales en R Studio, un diseño de 1 factor, 1 diseño en bloques y 1 diseño de 2 factores aleatorios.

## Resultados

Los análisis realizados mediante la metodología de diseño de experimentos evidencian que el área de adscripción funcional dentro de la organización tiene un efecto estadísticamente significativo sobre el nivel de madurez. Las áreas de Notificaciones y Desarrollos Tecnológicos presentaron los mayores niveles de madurez (84.9% y 82.3%, respectivamente), en contraste con la Unidad Administrativa y el área de Facturación, que registraron los niveles más bajos. Estos hallazgos sugieren la existencia de brechas organizacionales internas que podrían incidir en la eficacia de las políticas de seguridad.

Asimismo, los resultados indican que el nivel de conocimiento sobre las temáticas evaluadas impacta significativamente en el nivel de madurez. Se observaron desempeños superiores en tópicos como redes sociales y buenas prácticas financieras, mientras que los dominios de amenazas latentes y dispositivos domóticos presentaron deficiencias generalizadas, lo cual pone en evidencia la necesidad de estrategias formativas focalizadas.

Por otro lado, se examinó el efecto de variables sociodemográficas como el tipo de vinculación laboral y el género. Si bien el tipo de vinculación no mostró una influencia significativa, el género sí presentó una diferencia estadísticamente significativa, con un desempeño levemente superior en los participantes de género masculino (75.7%), aunque este hallazgo debe interpretarse con cautela y en el marco de futuras investigaciones.

## Conclusiones

Esta investigación aporta evidencia empírica sobre los factores que inciden en el nivel de madurez en seguridad de la información dentro del sector público, y destaca el valor del diseño experimental como herramienta metodológica rigurosa para la evaluación de políticas y estrategias institucionales en entornos digitales. Los resultados permiten orientar intervenciones más eficaces y adaptadas al perfil organizacional, contribuyendo al fortalecimiento de una cultura de seguridad integral y sostenida.

## Referencias


Hochstetter-Diez, J., Diéguez-Rebolledo, M., Fenner-López, J., & Cachero, C. (2023). AIM Triad: A Prioritization Strategy for Public Institutions to Improve Information Security Maturity. *Applied Sciences*, *13*(14), 8339. https://doi.org/10.3390/app13148339

Jevtić, N., & Alhudaidi, I. (2023). The importance of information security for organizations. *Serbian Journal of Engineering Management*, *8*(2), 48–53. https://doi.org/10.5937/SJEM2302048J

Samara, N. K. (2023). Cybersecurity Requirements for Management Information Systems. *Journal of Information Security*, *14*(03), 212–226. https://doi.org/10.4236/jis.2023.143013