Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

MODELO DE GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN COBIT 5 PARA LA MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN EN LAS UNIVERSIDADES

INFORMATION TECHNOLOGY GOVERNANCE MODEL BASED ON COBIT 5 FOR IMPROVING INFORMATION SECURITY IN UNIVERSITIES

Isis Ayme Moran Temoche
Universidad Ncional Federico Villareal – Perú

Ciro Rodriguez Rodriguez
Universidad Ncional Federico Villareal - Peru

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22825

Modelo de gobierno de tecnologías de información basado en COBIT 5 para la mejora de la seguridad de la información en las universidades

Isis Ayme Moran Temoche[1]
ayme_mt@hotmail.com
https://orcid.org/0009-0003-3076-241X
Universidad Ncional Federico Villareal
Perú

Ciro Rodriguez Rodriguez
crodriguez@unfv.edu.pe
https://orcid.org/0000-0003-2112-1349
Universidad Ncional Federico Villareal
Peru

RESUMEN

Esta investigación tuvo como objetivo desarrollar determinar en qué manera el diseño de un MGTI basado en COBIT 5 mejora la SI en las universidades. Este estudio surgió por la creciente dependencia de las instituciones universitarias de las tecnologías de la información y el incremento de incidentes de seguridad que afectan la seguridad de la información, fue del tipo cuasi experimental donde se realizaron pruebas orientadas a contrastar cada uno de los objetivos específicos del estudio, sobre una muestra conformado por 30 procesos para evaluar la efectividad del Modelo de Gobierno de Tecnologías de la Información (MGTI) basado en COBIT 5 en la mejora de la seguridad de la información en las universidades. De los resultados consolidados de los seis indicadores muestran diferencias estadísticamente significativas ($p < 0,05$) entre el grupo control y el grupo experimental, se acepta la hipótesis general, ya que la aplicación del MGTI bajo COBIT 5 mejoró significativamente la seguridad de la información y la capacidad de respuesta institucional, asegurando la Confidencialidad, Integridad y Disponibilidad de los activos informáticos. Se concluye que el diseño de un MGTI basado en COBIT 5 mejora la SI en las universidades mejora significativamente la SI en las universidades, donde, esta afirmación se sustenta con las pruebas de evaluación y validación realizadas, las mismas que sostienen resultados eficientes y de acorde a los objetivos e hipótesis de estudio.

Palabras claves: gobierno de tecnologías de información; cobit 5; seguridad de la información; incidentes de seguridad

[1] Autor Principal
Correspondencia: ayme_mt@hotmail.com

Information technology governance model based on COBIT 5 for improving information security in universities

ABSTRACT

This research aimed to determine how the design of an IT Governance Model (IGM) based on COBIT 5 improves information security in universities. This study arose from the growing dependence of universities on information technologies and the increase in security incidents affecting information security. It was a quasi-experimental study in which tests were conducted to compare each of the specific objectives of the study on a sample of 30 processes to evaluate the effectiveness of the IT Governance Model (IGM) based on COBIT 5 in improving information security in universities. The consolidated results of the six indicators show statistically significant differences ($p < 0.05$) between the control group and the experimental group. The general hypothesis is accepted, as the application of the IGM under COBIT 5 significantly improved information security and institutional response capacity, ensuring the confidentiality, integrity, and availability of IT assets. It is concluded that the design of an IT Governance Management System (IGMS) based on COBIT 5 significantly improves Information Security (IS) in universities. This assertion is supported by the evaluation and validation tests performed, which demonstrate efficient results consistent with the study's objectives and hypotheses.

Keywords: information technology governance; cobit 5; information security; security incidents

Artículo recibido 10 diciembre 2025
Aceptado para publicación: 10 enero 2026

INTRODUCCIÓN

Actualmente el auge de la TI ha tenido un impacto significativo en nuestra forma de vida. Para Mangalaraj et al. (2014), en la actualidad se necesita un marco integral que cubra todos los aspectos de TI debido a varias razones, como la necesidad implementar recursos de TI de manera efectiva, crear controles internos adecuados y prevenir problemas relacionados con errores de software. La gobernanza de TI es esencial para que las universidades brinden educación de calidad, realicen investigaciones innovadoras y administren sus procesos. Determinar los mecanismos de TI adecuados sigue siendo una tarea compleja. Los estudios previos se concentraron en los mecanismos de gobernanza de TI (Pereira et al., 2014).

En la actualidad, las universidades operan en un entorno caracterizado por el aumento de la dependencia de las funciones sustantivas en las Tecnologías de la Información. Esta tendencia ha elevado el nivel de complejidad de la gestión tecnológica y ha desafiado las nuevas amenazas a la seguridad de la información, especialmente en los casos en que no se desarrolla ningún modelo formal del gobierno de TI. Por lo general, las responsabilidades de gestión tecnológica en una institución de educación superior se enfocan en la operación de los servicios tecnológicos y no abarcan la alineación institucional, la gestión de riesgos ni el control del desempeño.

Bajo este marco, las universidades no pueden prever y evitar los riesgos de seguridad de la información y están expuestas al fraude, la modificación o la denegación de accesos. En ese sentido, el desarrollo de una estructura de marco de gobierno y gestión COBIT 5 que ayude a abordar estas preocupaciones o retos de manera sistemática y orientada con la estrategia y la orientación de riesgo. De acuerdo con ISACA (2019), a pesar de que la SI para las universidades debe ser lo más importante, existen desafíos que impiden su adecuada implementación, en primer lugar la falta de una cultura de seguridad entre los usuarios y administradores de TI que no son conscientes de las inseguridades a los que enfrentan a los sistemas de sus instituciones , la segunda es la falta de inversión en seguridad para la información ya que suelen destinar pocos recursos en seguridad de la información, lo que les hace que estés expuesto a los ataques. Es importante señalar de acuerdo con Seclén (2016), cada vez es mayor la exposición de las organizaciones y sus estructuras a los riesgos e incertidumbre procedentes de diversas fuentes como espionaje, fraude, algunas fuentes de daños como los virus y negación de servicios se están adquiriendo

un carácter cada vez más habitual y previsible.

Este estudio se efectúa con la finalidad de cooperar con nuevos datos sobre como el gobierno de TI permite agregar valor a las universidades y que logren mejores estrategias acordes a sus objetivos establecidos enfocándolo en salvaguardar la data, que actualmente es un punto decisivo para cualquier tipo de organización. Debido a una necesidad actual de las universidades, debido a que no aprovechan el valor de las TI y a su vez descuidan la protección sobre la data sensible y en general que se maneja en ellas, es por eso que un GTI permitirá ampliar los objetivos, aprovechar las TI y alinearlos a las estrategias de la empresa y también a tener un mejor manejo en la seguridad de información permitiendo que la data esté resguardada y protegida ante cualquier eventualidad que pueda presentarse.

Para Huamán (2021), en su investigación “Diseño de un Modelo de Gobierno de TI basado en COBIT 5 para mejorar la seguridad de la base de datos en la Municipalidad Distrital de Ascensión”, demuestra que la aplicación de este marco tiene una influencia positiva significativa sobre la seguridad de la información. Mediante una metodología cuantitativa con enfoque correlacional, se evidenció que existe una relación del 79.5% entre el Gobierno de TI basado en COBIT 5 y la mejora en la protección de las bases de datos. El estudio permitió identificar que la implementación de políticas, controles y procesos de gobernanza específicos contribuyen a disminuir riesgos y fortalecer la integridad, confidencialidad y disponibilidad de la información en el entorno municipal.

(Pérez-García et al., 2022), en su artículo “MGTI basado en COBIT 5 para la mejora de la SI en una empresa de servicios financieros", la investigación integró entrevistas semiestructuradas, sesiones de grupos focales y revisión documental. La investigación parte de una definición operativa de SI, entendiéndola como el conjunto de mecanismos orientados a preservar la confidencialidad, integridad y disponibilidad de los datos, previniendo pérdidas, accesos no autorizados, divulgaciones indebidas, modificaciones no deseadas o destrucción de la información.

Aquino et al. (2023), en el artículo “El modelo COBIT 5 para Auditoría Informática de los Sistemas de Información Académica de la Universidad Nacional Jorge Basadre Grohmann”, señalan que COBIT 5 permite establecer un marco de referencia integral que contribuye al control, mejora continua y excelencia operativa de los sistemas de información. Su estudio resalta que, mediante la aplicación de COBIT 5, se logra alinear las tecnologías con los objetivos institucionales, integrando políticas claras,

buenas prácticas y una visión de alto nivel orientada al negocio. Además, destacan que este modelo permite mantener la información de alta calidad, optimizar los servicios tecnológicos, gestionar los riesgos de TI y apoyar el cumplimiento normativo, consolidando así un gobierno de TI robusto y confiable en contextos académicos.

Este trabajo de investigación se tiene como hipótesis que el diseño de un MGTI basado en COBIT5 mejora significativamente la SI en las universidades; y el objetivo principal es determinar si el diseño de un MGTI basado en COBIT 5 mejora la SI en las universidades.

METODOLOGÍA

La presente investigación es de tipo aplicada, de acuerdo a (Hernández et al., 2014), este tipo de investigación construye, transforma y se utiliza en una práctica determinada para resolver problemas concretos de la realidad. Se basa en el conocimiento existente, pero también genera nuevo conocimiento para abordar los problemas.

El nivel de la investigación es descriptivo y explicativo, Se utiliza el diseño cuasi experimental, se toma una muestra de 30, se emplea el procedimiento de observación por medio del instrumento guía de observación para la obtención de la data para la investigación. Se realiza el análisis de datos cuantitativos de manera automatizada y/o computarizada utilizando Microsoft Excel y el paquete estadístico computacional SPSS, para obtener como resultados, las correlaciones existentes entre las variables.

Los instrumentos de recolección de datos son guías de observación las cuales se detallan a continuación:

Tabla 1. Guía 1 - Número de IDS reportados (NISR)

Fecha	Observación / Descripción del incidente	Unidad observada (sistema/área afectada)	Incidente reportado

Tabla 2. Guía 2 - Porcentaje de Accesos No Autorizados (%ANA)

Fecha	Número total de acceso	Número de accesos no autorizados detectados	% accesos no autorizados

Tabla 3. Guía 3 - Porcentaje de riesgos mitigados (PRM)

Fecha	Número total riesgos identificados	Número de riesgos mitigados	% de riesgos mitigados

Tabla 4. Guía 4 - Porcentaje de incidentes que afectan la integridad (%IDS) -

Fecha	Incidentes de seguridad	Incidentes con impacto de integridad	% incidentes con impacto en integridad

Tabla 5. Guía 5 - Tiempo medio de respuesta ante IDS

Fecha	Tiempo total de respuesta	Incidentes atendidos	Tiempo de respuesta

Tabla 6. Guía 6 - Porcentaje de Interrupciones del servicio

Fecha	Número total de horas de servicio	Número de interrupciones del servicio	% interrupciones del servicio

RESULTADOS

Se contrastaron las hipótesis formuladas al inicio de la investigación, con base en los resultados obtenidos de las guías de observación aplicadas antes y después de la implementación del Modelo de Gobierno de Tecnologías de Información (MGTI) basado en COBIT 5.

Hipótesis General

Hipótesis: La aplicación del Modelo de Gobierno de Tecnologías de Información (MGTI) basado en COBIT 5 mejora la gestión de la seguridad de la información en las universidades, reduciendo los incidentes de seguridad y mejorando la confidencialidad, integridad y disponibilidad de los datos.

La Comprobación de los resultados consolidados de los seis indicadores muestran diferencias estadísticamente significativas ($p < 0,05$) entre el grupo control y el grupo experimental.

Después de la implementación del MGTI:

- Los incidentes de seguridad (NISR) y accesos no autorizados (%ANA) disminuyeron en más del 60%.
- El porcentaje de riesgos mitigados (PRM) aumentó de forma notable, mientras que los incidentes que afectaron la integridad (%IDS) se redujeron más del 50%.
- El tiempo medio de respuesta (TMR) y las interrupciones del servicio (%IS) también descendieron significativamente más de 40%, fortaleciendo la disponibilidad operativa.

Tabla 7. Resumen general de indicadores por variable e hipótesis comprobada

Variable	Indicadores	Comportamiento post implementación	Resultado	p-valor
Independiente (MGTI basado en COBIT 5)	X1: NISR	NISR ↓ / PRM ↑ / TMR ↓	Mejora significativa	$p < 0,05$
	X2: PRM			
	X3: TMR			
Dependiente (Seguridad de la información)	Y1: %ANA	%ANA ↓ / %IDS ↓ / %IS ↓	Mejora significativa	$p < 0,05$
	Y2: %IDS			
	Y3: %IS			

Nota. Elaboración propia

La Conclusión es que se acepta la hipótesis general, ya que la aplicación del MGTI bajo COBIT 5 mejoró significativamente la seguridad de la información y la capacidad de respuesta institucional, asegurando la Confidencialidad, Integridad y Disponibilidad (CDI) de los activos informáticos.

Hipótesis específicas

H1: La aplicación del MGTI basado en COBIT 5 reduce los incidentes de seguridad y accesos no autorizados.

- Comprobación: NISR y %ANA disminuyeron significativamente ($p < 0,05$).
- Conclusión: Se acepta H1.

H2: La aplicación del MGTI basado en COBIT 5 incrementa el porcentaje de riesgos mitigados y reduce los incidentes que afectan la integridad.

- Comprobación: PRM aumentó mientras %IDS disminuyó ($p < 0,05$).
- Conclusión: Se acepta H2.

H3: La aplicación del MGTI basado en COBIT 5 disminuye el tiempo medio de respuesta y el porcentaje de interrupciones del servicio.

- Comprobación: TMR y %IS se redujeron significativamente ($p < 0,05$).
- Conclusión: Se acepta H3.

Tabla 8. Resumen de comprobación de hipótesis específicas

H	Indicadores asociados	Variable evaluada	Resultado observado	Prueba estadística aplicada	p-valor	Decisión
H1	X1: Número de incidentes de seguridad reportados (NISR) Y1: % de accesos no autorizados (%ANA)	Confidencialidad de la información (CDI)	NISR ↓ 60% %ANA ↓ 66%	Mann–Whitney y t de Welch	p < 0,05	Se acepta H1
H2	X2: % de riesgos mitigados (PRM) Y2: % de incidentes que afectan la integridad (%IDS)	Integridad de la información (IDI)	PRM ↑ significativo %IDS ↓ >50%	t de Welch / U de Mann–Whitney	p < 0,05	Se acepta H2
H3	X3: Tiempo medio de respuesta (TMR) Y3: % de interrupciones del servicio (%IS)	Disponibilidad de la información (DDI)	TMR ↓ significativo %IS ↓ >40%	t de Welch / U de Mann–Whitney	p < 0,05	Se acepta H3

Nota.. El nivel de significancia se estableció en $\alpha = 0,05$, considerando diferencias significativas cuando $p < 0,05$.

Se concluye El contraste de hipótesis evidencia que el MGTI basado en COBIT 5 influyó positivamente en todas las dimensiones de la seguridad de la información:

- Confidencialidad: se fortaleció con la reducción de accesos no autorizados.
- Integridad: mejoró con la mitigación de riesgos y la disminución de incidentes que alteran los datos.
- Disponibilidad: se incrementó al reducir el tiempo medio de respuesta y las interrupciones del servicio.

Los resultados obtenidos confirman empíricamente la efectividad del modelo MGTI basado en COBIT 5 en la gestión integral de la seguridad de la información, sustentando la aceptación de todas las hipótesis planteadas.

DISCUSIÓN

La investigación tuvo como problema general conocer ¿de qué manera el diseño de un Modelo de Gobierno de Tecnologías de Información (MGTI) basado en COBIT 5 mejora la seguridad informática en las universidades?, y como hipótesis general se planteó que el diseño de un MGTI basado en COBIT 5 mejora significativamente la seguridad informática en las universidades.

Ahora bien, los resultados obtenidos confirman la hipótesis general planteada, evidenciando una

correlación fuerte y significativa entre la implementación del MGTI y la mejora de la seguridad de la información, con un grado de confiabilidad promedio de 87%. Los hallazgos se sustentan en las tres dimensiones de la seguridad informática, es decir, la confidencialidad, la integridad y la disponibilidad (CID), corroboradas a través de los seis indicadores aplicados en las guías de observación.

En el análisis de la confidencialidad de la información (CDI), se observó una reducción significativa de los incidentes de seguridad (NISR) y del porcentaje de accesos no autorizados (%ANA) tras la implementación del modelo. Este resultado coincide con lo propuesto por Gaspar (2020), quien demostró que la adopción de COBIT 5 como marco de gobierno de TI corrige deficiencias en infraestructura y control de datos, fortaleciendo la protección frente a accesos indebidos.

Asimismo, Schicht (2021) destaca que las organizaciones que implementan modelos de gobierno de TI basados en COBIT obtienen un manejo más eficiente de incidentes y una reducción en violaciones de seguridad, lo que coincide directamente con los resultados alcanzados en esta investigación.

Respecto a la integridad de la información (IDI), el estudio evidenció un aumento del porcentaje de riesgos mitigados (PRM) y una disminución significativa de los incidentes que afectan la integridad (%IDS). Estos hallazgos reafirman lo señalado por Oñate (2022), quien plantea que una gobernanza efectiva de TI mejora la calidad del servicio y la gestión de riesgos mediante el principio de responsabilidad institucional. De manera similar, en esta investigación, la implementación del MGTI promovió políticas y controles alineados con APO12 - Gestionar el riesgo y DSS05 - Gestionar los servicios de seguridad, que contribuyeron a mitigar vulnerabilidades críticas y reforzar la integridad de los activos digitales.

En relación con la disponibilidad de la información (DDI), los resultados demostraron una reducción significativa del tiempo medio de respuesta (TMR) y del porcentaje de interrupciones del servicio (%IS), lo que fortaleció la continuidad operativa, coincidiendo estos resultados con lo descrito por Huamán (2021), quien sostiene que el Gobierno de TI basado en COBIT 5 impacta positivamente en la seguridad de la información al establecer políticas y procesos que minimizan las interrupciones y aseguran la disponibilidad de los servicios.

En la presente investigación, la aplicación de los procesos DSS02 - Gestionar incidentes y DSS04 - Garantizar la continuidad del servicio permitió optimizar la atención y recuperación ante fallas,

garantizando la estabilidad de las operaciones institucionales. En conjunto, los resultados empíricos y estadísticos demuestran que el MGTI basado en COBIT 5 influyó de manera positiva, significativa y coherente con los principios del marco teórico, alcanzando mejoras cuantificables en los seis indicadores medidos.

Estos resultados validan el modelo propuesto como una herramienta eficaz para la gestión estratégica de la seguridad informática en entornos universitarios, consolidando una cultura organizacional orientada a la prevención, control y mejora continua.

CONCLUSIONES

Se desarrolló un MGTI basado en COBIT 5 para mejorar la seguridad de la información en las universidades. Este permitió reducir los accesos no autorizados, disminuir los incidentes de seguridad (IDS) y optimizar la respuesta ante interrupciones del servicio. En conjunto, la investigación demuestra que la implementación del modelo contribuye significativamente con la seguridad de la información en las universidades.

Se redujeron los incidentes de seguridad (NISR) y el porcentaje de accesos no autorizados (%ANA) mediante la aplicación del MGTI basado en COBIT 5, sustentado en los procesos APO13 - Gestionar la seguridad y DSS02 - Gestionar incidentes. El análisis estadístico evidenció una disminución superior al 60 % en ambos indicadores, confirmando que la implementación del modelo fortalece la confidencialidad de la información institucional.

Se incrementó el porcentaje de riesgos mitigados (PRM) y se redujeron los incidentes que afectan la integridad (%IDS), alcanzando una confiabilidad del 87%. Los resultados reflejan que la adopción del modelo MGTI basado en COBIT 5, a través de los procesos APO12 - Gestionar el riesgo y DSS05 - Gestionar los servicios de seguridad, mejoró sustancialmente la gestión del riesgo tecnológico y la preservación de los datos.

Se disminuyó el tiempo medio de respuesta (TMR) y el porcentaje de interrupciones del servicio (%IS), con un nivel de confiabilidad del 87,5%, evidenciando la efectividad de los procesos DSS02 - Gestionar incidentes y DSS04 - Garantizar la continuidad del servicio. Esta mejora demuestra que el modelo propuesto fortalece la disponibilidad operativa de los sistemas y la capacidad de recuperación ante incidentes.

REFERENCIAS BIBLIOGRÁFICAS

Amenazas informáticas. [sitio web]. 2015 [consulta 25 enero 2017]. Disponible en: forma.kzgunea.eus/mod/book/view.php?id=5800&chapterid=7518

ASHRAF, Javed 2010 “Why do Public Sector IT Projects Fail”. The 7th International Conference on Informatics and Systems (INFOS), 2010. Cairo, pp 1-6

COBIT (2012), Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. capítulo de Madrid ISACA®. España

DeNardis, 2007 “Una historia de la seguridad en Internet”, La historia de la seguridad de la información: un manual completo, Elsevir, 2007.

Durán, D. (2002). Epistemología y metodología de la investigación social. Madrid, España: McGraw-Hill.

García, J., López, M., y Rodríguez, J. (1997). Investigación educativa: fundamentos y técnicas. Madrid: McGraw-Hill.

García, M. (2018). Gobierno de las tecnologías de la información: un enfoque integral. Madrid: ESIC Editorial.

Godoy, J. (2014). Seguridad de Información: Una visión integral. Revista de Contabilidad y Administración, 59(1), 1-22.

Grembergen, W. van. (2002). IT Governance: A Framework for Alignment, Risk Management and Performance Improvement. Long Range Planning, 35(6), 5-22.

Hamati-Ataya, I. (2012). Reflectivity, reflexivity, reflexivism: IR's 'reflexive turn'—and beyond. European Journal of International Relations, 19(4), 669-694.

Isaca. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. Rolling Meadows, IL: ISACA

ISACA. (2019). COBIT 5: A business framework for the governance and management of enterprise

Mangalaraj George, Singh Anil, Taneja Aakash. 2014 “Marcos de gobierno de TI y COBIT”, Vigésima Conferencia de las Américas sobre Sistemas de Información, Savannah, 2014

Oñate, A. (2022). Contribuciones al gobierno de las tecnologías de la información en el contexto universitario. Universidad Mayor de San Marcos.

Oñate-Andino, A., & Mauricio, D. (2019). The advances of information technology governance in universities: A systematic review. Journal of Theoretical and Applied Information Technology, 97(21), 3084–3109.

Ozdemir, O., Ozturk, A., & Demirtas, A. (2018). Evaluation and comparison of the COBIT, ITIL and ISO27K1/2 standards within the information security framework. Security and Privacy, 16(2), 21-32.

Pelanda, M. L. (2006). Modelos de governança de tecnologia da informação adotados no Brasil :um de casos múltiplos. Tesis Magíster, Universidade Metodista de São Paulo, São Paulo

Pereira, R., Almeida, R. y Silva, M. 2014b. "Patrones de gobernanza de TI en la industria financiera portuguesa",Ciencias de Sistemas (HICSS), 2014 47a Conferencia Internacional de Hawaii sobre, págs. 4386-4395.

Pérez-García, M. J., García-Cuesta, J. J., & González-Gutiérrez, R. (2022). Modelo de gobierno de TI basado en COBIT 5 para la mejora de la seguridad de la información en una empresa de servicios financieros. International Journal of Information Management, 60, 102469.

Quiroz Silvia, Macías David. [sitio web]. 2017 “Computer security: considerations”. Disponible en http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.5.agos.676-688

Sánchez, R., Reyes, A., & Mejía, J. (2018). Niveles de investigación: Descriptivo, Explicativo y Predictivo. Revista de Investigación en Ciencias Sociales, 14(2), 123-136.

Seclén, J. (2016). Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001. Recuperado de https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/4884/Seclen_aj.pdf?sequence=3 TI.pdf

Van Grembergen, W., & De Haes, S. (04 de January de 2017). Introduction to IT Governance and its Mechanisms Minitrack. doi:10.24251/HICSS.2017.626