Propósitos y Representaciones
ISSN 2307-7999
e-ISSN 2310-4635

Sep.-Dec. 2020, Vol. 8, N° 3, e786
Monographic: Educational management and teaching skills
http://dx.doi.org/10.20511/pyr2020.v8n3.786

RESEARCH NOTES

Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana

Application of ISO 27001 and its influence on the information security of a Peruvian private company

Liset Sulay Rodriguez Baca
Universidad César Vallejo, Lima, Perú
ORCID: https://orcid.org/0000-0003-1850-615X

Carlos Francisco Cruzado Puente de la Vega
Universidad César Vallejo, Lima, Perú
ORCID: https://orcid.org/0000-0001-7471-3140

Carolina Mejía Corredor
Universidad EAN, Colombia
ORCID: https://orcid.org/0000-0002-3560-5443

Mitchell Alberto Alarcón Diaz
Universidad César Vallejo, Lima, Perú
ORCID: https://orcid.org/0000-0003-0027-5701

Received 03-24-20 **Revised** 05-30-20 **Accepted** 08-08-20 **On line** 10-27-20

***Correspondence**

Email: lrodriguezb@ucv.edu.pe

Cite as:

Rodriguez Baca, L., Cruzado Puente de la Vega, C., Mejía Corredor, C., & Alarcón Diaz, M. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones, 8*(3), e786. doi: http://dx.doi.org/10.20511/pyr2020.v8n3.786

Resumen

El avance de la tecnología en el mundo provoca, entre otros aspectos, el manejo de importante información la misma que puede considerarse como fundamental para los intereses estratégicos de las empresas. La investigación tuvo como objetivo el analizar la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada de Lima (Perú). A partir de la aplicación de una metodología cuantitativa, se empleó un estudio pre experimental en el que se determinó la influencia de la aplicación del ISO 27001.Para ello se consideró a una muestra de 30 colaboradores de la empresa. La conclusión cuantitativa muestra que si existe una influencia de la aplicación del ISO en la seguridad de la información y en las dimensiones confidencialidad, integridad y disponibilidad.

Palabras clave: Confidencialidad de datos, privacidad de los datos, disponibilidad de la información, seguridad de la información, tecnología e información

Summary

The advancement of technology in the world causes, among other aspects, the handling of important information, which can be considered as fundamental for the strategic interests of companies. The objective of the research was to analyze the influence of the application of ISO 27001 on the information security of a private company in Lima (Peru). Based on the application of a quantitative methodology, a pre-experimental study was used in which the influence of the application of ISO 27001 was determined. To this end, a sample of 30 employees of the company was considered. The quantitative conclusion shows that there is an influence of the application of ISO on information security and the dimensions of confidentiality, integrity and availability.

Keywords: Data confidentiality, data privacy, information availability, information security, technology and information

Introducción

La realidad problemática relacionada a la investigación involucró al hecho que diferentes empresas invierten su presupuesto en la implantación de Sistemas informáticos con el fin de dar soporte a sus procesos de negocios y liderar en un mercado cada vez más competitivo y de constante cambio tecnológico.

Según Calder y Watkins (2019) sostienen que las organizaciones, en su mayoría consideran presupuesto para invertir sistemas de información para posicionarse en el mercado, buscar la excelencia operacional, incursionar en nuevos modelos de negocios, cercanía con los clientes y proveedores, ventaja competitiva frente a sus competidores; todo ello está basado en el adecuado manejo de la información que ayude a tomar decisiones estratégicamente.

De acuerdo a lo descrito en líneas anteriores, la información física y digital desempeña un rol importante ya que es el activo clave de toda organización. Si una empresa no administra adecuadamente su información, estará altamente vulnerable a los riesgos lo que podría afectar la continuidad del negocio. Por ello, es importante que se establezca mecanismos de seguridad para proteger la información (Gómez y Católico, 2010).

Laudon y Laudon (2016) y Miguel (2015) afirman que el control y la seguridad inadecuada puede generar inconvenientes de tipo legal; por ello es importante que las empresas implementen mecanismos o estrategias no solo para proteger su información sino también la de sus clientes, colaboradores, socios estratégicos. Ya que, al carecer de mecanismos de seguridad, las organizaciones se encuentran vulnerables y puede ser responsables de crear riesgos de alto impacto, daños innecesarios causando pérdida de información confidencial (Mariño y Alfonzo, 2019).

Es por ello, que es de total relevancia que toda información debe ser protegida pero también debe estar disponible para ser accedida oportunamente. Considerando el enfoque de la seguridad de la información es necesario considerar tres elementos fundamentales como son: la confidencialidad, integridad y disponibilidad. Muchas organizaciones han implementado políticas, acciones necesarias para evitar el robo o manipulación de su información, pero con la constante evolución tecnológica se han incrementado los riesgos, vulnerabilidades, amenazas a las que se ven expuestas.

Asimismo, en el Perú, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) ha publicado en su página web y en el Diario Oficial El Peruano reglamentos, normas referentes a la seguridad de la información con el fin de sugerir a las empresas estatales a proteger el activo sensible mediante de un sistema de gestión de seguridad de la información, lo que también se puede contextualizar a empresas privadas.

Con el desarrollo de la investigación, se logró identificar la influencia de la aplicación de las normas ISO 27001 en la seguridad de la empresa en cuestión; esto se concretó a través de un análisis estadístico y, como una forma de complementar estos hallazgos, se conoció el punto de vista de los expertos acerca de las características que tiene esa influencia.

Fundamento

La importancia de este estudio radica en el diagnóstico acerca de la seguridad en espacios en los que se maneja información neurálgica al interior de las instituciones. El objetivo propuesto fue el

analizar la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada de Lima (Perú). Acerca de ello, se puede afirmar que la norma ISO abarcan la seguridad de la información (Espinoza, 2019). De manera retrospectiva, su origen va desde el año 1995 (Valencia-Duque y Orozco - Alzate, 2017). Hacia el año 1999 se crearon nuevos estándares orientados a las buenas experiencias en gestión de seguridad y normas para la gestión de riesgos. Entre los años 2001 al 2004 se revisaron y actualizaron las ISO/IEC las que se difundieron en el año 2005. El éxito de la aplicación de la implementación no solo depende de la calidad de la norma sino del involucramiento de los colaboradores (Martínez, 2017). La buena práctica de la gestión de la seguridad reduce el impacto de la vulnerabilidad de la información perteneciente a la empresa.

Estudios previos realizados evidencian la importancia de la temática abordada. Santos (2016) realizo un estudio relacionado con el entorno de riesgos en una empresa consultora de software, para ello empleo la metodología Margerit; el investigador concluyó que la empresa exitosa depende de insumos diversos, entre ellos la elaboración de dispositivos apropiados y que a su vez cumplan con las exigencias del ISO 27001. Por su parte Talavera (2015) y Vilca (2017) diseñaron modelos de gestión de la seguridad en los que se aplicaron la metodología de análisis de riesgos, la metodología de valoración de activos teniendo como conclusión que las implementaciones de los sistemas de gestión de la seguridad de la información determinan los riesgos al interior de una empresa.

Andrade y Chávez (2018) a través de un estudio enfocado en la mejora de los procesos a través de la norma ISO 27001 determinó que, ante factores de riesgo existente, los planes de mejora garantizan los aspectos de integridad, disponibilidad y accesibilidad. Arlenys (2017) desarrolló una investigación basada en un trabajo de campo dividido en tres momentos: la planificación, preparación y la capacitación - concientización. A partir de esa intervención se logró disminuir los niveles de riesgo en la empresa, se empleó la norma ISO 27001: 2013.

Esta investigación presenta una relevancia teórica ya que se pone a prueba los criterios bajo los cuales se maneja la información al interior de una empresa y para lo cual se emplea una norma de calidad ISO. En el aspecto práctico, este estudio analizó estadísticamente la influencia de la norma y de manera prospectiva se sugiere consideraciones para una mejor aplicabilidad de la misma.

Metodología

La investigación fue de tipo mixta, al respecto Ñaupas, Mejia, Novoa y Villagomez, 2018) comenta que el estudio aplicado prevalece el factor práctico que se sustenta en la teoría. El diseño

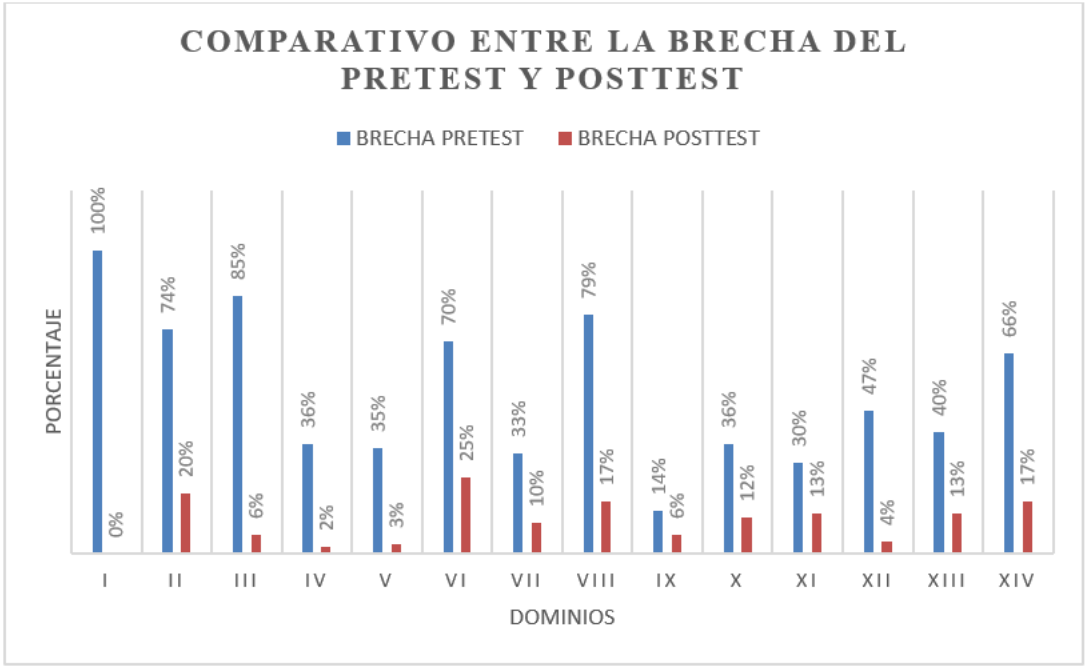
empleado fue el preexperimento; se consideró a 30 colaboradores a los que se evaluó antes y después de la intervención realizada. La técnica de la observación permitió verificar el cumplimiento de la norma ISO y a través del instrumento de la lista de cotejo se recopiló la información. Se seleccionó la muestra teniendo en cuenta la técnica de muestreo por conveniencia. Luego se aplicó una lista de cotejo que permitió registrar los diversos valores de los ítems de la lista de cotejo en el pre y postest, basado en el ISO 27001 e ISO 27002.

En la investigación se empleó la técnica de la observación y la entrevista, y como instrumento, la lista de cotejo, esta sirvió para reunir y registrar los datos, que a su vez le otorgan unidad y valor propio. Los investigadores realizaron trabajo de campo en una empresa privada ubicada en un distrito limeño, para desarrollar las actividades propuestas en la implementación o aplicación del ISO 27001, los catorce dominios y los objetivos de control considerados con el fin de poder hacer la medición del pre y post test; los dominios considerados fueron: la organización de la seguridad de la información, seguridad de los recursos humanos, gestión de activos, control de acceso, criptografía, seguridad física y del entorno, seguridad de las operaciones, seguridad de las comunicaciones, adquisición, desarrollo y mantenimiento de sistemas, relaciones con los proveedores, gestión de incidentes de seguridad de la información, aspectos de seguridad de la información y finalmente, el cumplimiento. Estos dominios están integrados en tres grandes dimensiones: confidencialidad, integridad y disponibilidad de la información.

Para el análisis cualitativo se incluyó una entrevista dirigida a expertos en seguridad informática. Las respuestas formuladas fueron sistematizadas en una matriz de convergencias y divergencias. El estadístico empleado fue la prueba de Wilcoxon la cual es un estadístico no paramétrico el que permite comparar el rango promedio de dos muestras relacionadas. El procedimiento seguido consideró la aplicación de la lista de cotejo basada en el ISO 27001 y que incluyó el diagnóstico de los catorce dominios y los objetivos de control, con el fin de poder hacer la medición del pre y post test.

Resultados

La experiencia se realizó en una empresa privada. Luego, se recolectaron datos mediante la aplicación de una lista de cotejo sobre dimensión de confiabilidad, integridad y disponibilidad.



Fuente: Elaboración propia

Figura 01. Comparativo de los resultados de la brecha de pretest y post test

En relación a los 14 dominios, los resultados muestran que en todos los casos se hallaron mejoras porcentuales después de aplicada la intervención (pos test).

Tabla 1

Promedio de rangos pre y pos test Seguridad de la información

Rangos

		N	Rango promedio	Suma de rangos
Seguridad de la información (post-test) – Seguridad de la información (pre-test)	Rangos negativos	0[a]	,00	,00
	Rangos positivos	12[b]		
	Empates	18[c]	4,50	36,00
	Total	30		

a. Seguridad de la información (post-test) < Seguridad de la información (pre-test)
b. Seguridad de la información (post-test) > Seguridad de la información (pre-test)
c. Seguridad de la información (post-test) = Seguridad de la información (pre-test)

Tabla 2

Estadísticos de prueba pre y pos test Seguridad de la información

	Seguridad de la información (post-test) - Seguridad de la información (pretest)
Z	-3,828[b]
Sig. asintótica (bilateral)	.005

a. Prueba de rangos con signo de Wilcoxon b. Se basa en rangos negativos

En lo que se refiere a la hipótesis de investigación, se obtuvo un valor de Z= -3,828 (valor de p= .005) puesto que el valor de p es inferior al 5% de significancia, ello permite concluir que existe influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada, 2019.

En la parte cualitativa, se formularon interrogantes a dos expertos para la comprensión de los hallazgos. Frente a la pregunta ¿cómo influye la aplicación del ISO 27001 en la confidencialidad de la seguridad de la información de una empresa privada?, los expertos manifestaron que Es necesario que las empresas protejan su información de sus competidores. La confidencialidad de la información es clave para el crecimiento y sostenibilidad de la empresa, por ello se debe prevenir la divulgación no autorizada de la información empresarial. Es relevante que las empresas grandes, medianas o pequeñas apliquen ISO 27001,27002 de acuerdo a su ámbito ya que esta norma orientará como manejar los aspectos de seguridad de la información y evaluarán su situación actual y como pueden ir evolucionando en el tiempo. Toda empresa posee información confidencial, por lo tanto, debe resguardarla hasta de sus propios colaboradores; ellos deben ser conscientes de lo relevante que es el adecuado manejo de la información que generar en sus labores diarias. Muchas empresas grandes, medianas y pequeñas aplican normas internacionales y con ello analizan su situación actual frente a una situación deseada, tomando como base los pilares de la seguridad informática como son la confidencialidad.

Con relación a la pregunta ¿cómo influye la aplicación del ISO 27001 en la integridad de la seguridad de la información?, los entrevistados afirmaron que al aplicar ISO 27001 en una organización, a través de los dominios de esta norma, se evalúa la integridad de la seguridad de la información, esto implica que deben existir mecanismos, políticas, directivas conocidas por los colaboradores de las diferentes áreas orientados a prevenir modificaciones no autorizadas de la información que se maneja.

Evidentemente, los resultados obtenidos en relación a la integridad de la seguridad de la información, validan lo expuesto anteriormente; ya que, si una organización no implementa políticas o normas para el desarrollo de sus procesos, éstos marcharán a la deriva y expuestos a altos riesgos. Asimismo, se menciona que la aplicación de ISO 27001 si influye en la integridad

de la información porque permite evaluar que estrategias, políticas, directivas se están aplicando para evitar que la información sea alterada sin autorización.

Finalmente, y a la consulta ¿cómo influye la aplicación del ISO 27001 en la disponibilidad de la seguridad de la información?, las afirmaciones revelan que el aplicar el ISO 27001 en una organización impacta en la disponibilidad de la seguridad de la información, ya que es uno de los pilares de la seguridad de la información y sostiene que es necesario que la información debe ser accedida por usuarios autorizados. Se comenta también que la información de la organización se encuentra vulnerable a ataques, modificaciones y otros tipos de daños. La disponibilidad hace referencia a que los datos, información debe estar a disposición de los usuarios de forma oportuna y según los privilegios o accesos que se les haya asignado.

En relación a los resultados obtenidos, se encontró la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada. Estudios como el de (ANDRADE C., y otros, 2018) refieren que la aplicación de planes de mejora garantiza la integridad, disponibilidad y accesibilidad de la información haciendo referencia al ISO 27001. En tal sentido, se demuestra que el estudio realizado posee una valía teórica y metodológica ya que se comprobó la eficiencia del modelo ISO en la solución y mejora continua de la seguridad de la información. Los sistemas de seguridad han ido progresando a través del tiempo. En ese contexto los sistemas ISO han ido aportando elementos importantes a la seguridad desde la planificación de la misma hasta el monitoreo permanente. La influencia existente permite establecer un horizonte seguro y confiable para los usuarios.

También en relación a los resultados específicos obtenidos, se encontró la influencia de la aplicación del ISO 27001 en la confidencialidad, integridad y la disponibilidad de la seguridad de la información de una empresa privada, se comprobó la existencia de esa influencia. Este hallazgo coincide con el estudio de (ALVARADO M., 2016) quien garantizo la confiabilidad, integridad y disponibilidad como una forma de protección de clientes y proveedores. El autor en mención, identifico que la aplicación la norma ISO reduce el costo de tiempo. En tal sentido, la seguridad de manera integra puede verse reflejada en la confidencialidad de la información; la reserva de los activos de la empresa se convierte en un componente esencial para el logro de los objetivos estratégicos ya que mucha de esa información será útil para la toma de decisiones. Con respecto a la integridad y la disponibilidad, el fácil acceso y la credibilidad de los recursos se convierte en una creciente demanda de usuarios y gestores. A partir de estos elementos, se garantiza la fluidez de la seguridad de la información.

Conclusiones

Se demostró la influencia de la aplicación del ISO 27001 en la seguridad de la información al

interior de la empresa. Asimismo, se encontró una significativa influencia en aspectos tales como la confidencialidad de la información, integridad de la información y finalmente la disponibilidad de la seguridad de la información. Cualitativamente y respecto a la confidencialidad, la información debe ser accedida sólo por los usuarios autorizados, considerando su rol o cargo en la organización. Para ello, la ISO 27001 brinda políticas que deben implementar con la finalidad de garantizar la confidencialidad de la seguridad de la información. Tambien en lo que se refiere a la integridad, es imprescindible proteger la información para evitar que sea modificado sin autorización asignada por la organización. ISO 27001 ayuda a implementar procedimientos para garantizar la integridad de la información. Por último, en el tema de la disponibilidad de la información, la información debe estar disponible permanentemente para dar soporte a la toma de decisiones de los usuarios correspondientes.

Referencias

Alvarado M., E. (2016). Propuesta para la implementación de un sistema de gestión de seguridad de la información aplicando la norma ISO 27001 para industrias. Ecuador: ALES.

Andrade C. y Chávez, C. (2018). Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía internacional GYM ECUAINTERGYM S.A. de la ciudad de Guayaquil. Recuperado de http://repositorio.ug.edu.ec/handle/redug/32606

Arlenys, C. (2017). Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO/IEC 27001:2013. Recuperado de http://repository.poligran.edu.co/handle/10823/994

Calder, A. y Watkins, S. (2019). Information Security Risk Management for ISO 27001/ISO 27002. United Kingdom: IT Governance Publishing Ltd.

Espinoza, M. (2019). Importancia de los modelos para el gobierno de la seguridad de la información en las empresas: una revisión sistemática de la literatura. Revista Espacios, 40 (25), 5-20. Recuperado de https://www.revistaespacios.com/a19v40n25/a19v40n25p05.pdf

Gómez, F. y Católico, D. (2010). Relación de la presentación de información de negocios on-line con las variables financieras en las empresas colombianas. Revista Facultad de Ciencias Económicas: Investigación y Reflexión, 18(1), 205-224. Recuperado de https://bit.ly/2RtJRp3

JAY, Devore. 2016. Probabilidad y Estadística para Ingeniería y Ciencias. México : Cengage Learning Eitores, 2016. ISBN: 9786075228280.

Laudon, K. y Laudon, J. (2016). Sistemas de información gerencial. México: Pearson Educación.

Mariño, S. y Alfonzo, P. (2019). Evidencias de Accesibilidad Web en la generación de sitios: Propuesta de un método. Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología, (23), 52-60. Recuperado de https://bit.ly/38mnnMs

Martínez, E. (2017). Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Enfoque UTE, 8 (Supl. 1), 107-121. https://dx.doi.org/10.29019/enfoqueute.v8n1.140

Miguel, P. (2015). Seguridad en los sistemas informáticos. España: RA-MA.

Ñaupas, H., Valdivia, M., Palacios, J. y Romero, H. (2018). Metodología de la Investigación Cuantitativa - Cualitativa y redacción de la tesis. Colombia: Ediciones de la U.

Santos, D. (2016). Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Perú.

Talavera, V. (2015). Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013. Perú.

Valencia-Duque, F. y Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, (22), 73-88. https://dx.doi.org/10.17013/risti.22.73-88

Vilca, E. (2017). Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima. Recuperado de https://bit.ly/2DWZXzr