

# FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA INDUSTRIAL

“IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE INFORMACIÓN BASADO EN LA ISO 27001:2013 PARA PROTEGER LA INFORMACIÓN DE LOS PROCESOS OPERATIVOS EN LA EMPRESA CORE BUSINESS CORPORATION SAC, LIMA - 2021.”

Tesis para optar el título profesional de:

INGENIERA INDUSTRIAL



**Autora:**

Lucero Alessandra Arana Walde

**Asesor:**

Mg. Ing. Iselli Josylin Nohely Murga Gonzalez

Lima - Perú

2021

## TABLA DE CONTENIDOS

DEDICATORIA .....	2
AGRADECIMIENTO .....	3
ÍNDICE DE TABLAS .....	8
ÍNDICE DE FIGURAS .....	9
RESUMEN .....	10
ABSTRACT .....	11
<b>I. CAPÍTULO. INTRODUCCIÓN.....</b>	<b>12</b>
I.1. Realidad problemática .....	12
I.2. Antecedentes.....	18
I.2.1. Antecedentes Internacional .....	18
I.2.2. Antecedentes Nacionales .....	20
I.2.3. Antecedentes Locales .....	21
I.3. Marco teórico.....	23
I.3.1. Sistema de Gestión .....	23
I.3.2. Sistema de Gestión de la Seguridad de la Información .....	24
I.3.3. ISO 27001:2013.....	24
I.3.4. Activo de información .....	26
I.3.5. Información .....	26
I.3.6. Análisis costo - beneficio .....	27
I.3.7. Metodología MAGERIT.....	28
I.3.8. Ciclo PHVA.....	29
I.4. Justificación.....	30
I.5. Perspectiva de términos.....	32
I.6. Formulación del problema.....	33
I.7. Problemas específicos .....	33
I.8. Objetivos .....	33
I.8.1. Objetivo general .....	33
I.8.2. Objetivos específicos .....	33
I.9. Hipótesis .....	34
I.9.1. Hipótesis general .....	34
I.9.2. Hipótesis específicas: .....	34
<b>II. CAPÍTULO. MÉTODO .....</b>	<b>36</b>
II.1. Tipo de investigación.....	36
II.1.1. Propósito .....	36
II.1.2. Enfoque.....	36
II.1.3. Diseño .....	36
II.2. Población y muestra.....	37
II.2.1. Población.....	37

II.2.2.	<i>Muestra</i> .....	37
II.3.	Técnicas, instrumentos y herramientas de recolección y análisis de datos .....	38
II.3.1.	<i>Técnicas</i> .....	38
II.3.1.1.	<i>La observación</i> .....	38
II.3.1.2.	<i>Revisión de documentos</i> .....	38
II.3.2.	<i>Instrumentos</i> .....	38
II.3.2.1.	<i>Matriz de consistencia</i> .....	38
II.3.2.2.	<i>Lista de verificación</i> .....	39
II.3.3.	<i>Herramientas</i> .....	39
II.3.3.1.	<i>Diagrama Gantt</i> .....	39
II.3.3.2.	<i>Matriz de riesgos de SI</i> .....	39
II.4.	Procedimiento .....	41
II.4.1.	<i>Diagrama Gantt</i> .....	43
II.5.	Método de análisis de datos.....	43
II.5.1.	<i>Validez</i> .....	44
Los 3 expertos fueron los siguientes: .....		44
II.5.2.	<i>Confiabilidad</i> .....	44
II.6.	Aspectos Éticos .....	44
<b>III.</b>	<b>CAPÍTULO. RESULTADOS</b> .....	<b>45</b>
III.1.	Objetivo 1. Elaborar el diagnóstico de la empresa.....	45
III.2.	Objetivo 2. Evaluar el análisis costo-beneficio para determinar la viabilidad de la implementación de la ISO 27001:2013. ....	47
III.3.	Objetivo 3. Elaborar el análisis de riesgo de seguridad de la información .....	50
III.3.1.	<i>Planear</i> .....	50
III.3.1.1.	<i>Contexto de la organización</i> .....	50
III.3.1.1.1.	Comprender la organización y su contexto.....	50
III.3.1.1.1.1.	Misión .....	50
III.3.1.1.1.2.	Visión.....	51
III.3.1.1.1.3.	Foda.....	51
III.3.1.1.2.	Comprender las necesidades y expectativas de las partes interesadas.....	53
III.3.1.1.3.	Determinar el alcance del sistema de gestión.....	54
III.3.1.1.4.	Sistema de gestión de seguridad de la información .....	54
III.3.1.2.	<i>Liderazgo</i> .....	55
III.3.1.2.1.	Liderazgo y compromiso.....	55
III.3.1.2.2.	Política .....	56
III.3.1.2.3.	Roles, responsabilidades y autoridades organizacionales .....	58
III.3.1.3.	<i>Planificación</i> .....	60
III.3.1.3.1.	Acciones para tratar los riesgos y las oportunidades.....	60
III.3.1.3.1.1.	Generalidades .....	60
III.3.1.3.1.2.	Valoración del riesgo de seguridad de la información .....	61
III.3.1.3.1.2.1.	Valorización de activos de información.....	61
III.3.1.3.1.2.2.	Análisis de riesgo .....	69

III.3.1.3.1.2.2.1.	Identificación de Amenazas y vulnerabilidades.....	69
III.3.1.3.1.2.2.2.	Cálculo de la Probabilidad .....	69
III.3.1.3.1.2.2.3.	Cálculo del Impacto .....	70
III.3.1.3.1.2.2.4.	Identificación de las Consecuencias.....	72
III.3.1.3.1.2.2.5.	Cálculo del Nivel de Riesgo.....	72
III.3.1.3.1.2.3.	Tratamiento del riesgo.....	72
III.3.1.3.1.2.3.1.	Nivel de riesgo aceptable .....	72
III.3.1.3.1.2.3.2.	Estrategias de tratamiento de riesgos .....	73
III.3.1.3.1.2.4.	Selección de controles de seguridad .....	83
III.3.1.3.2.	Objetivos de seguridad de la información y planificación para conseguirlos .	93
III.3.1.4.	<i>SopORTE</i> .....	94
III.3.1.4.1.	Recursos .....	94
III.3.1.4.2.	Competencia .....	94
III.3.1.4.3.	Concientización.....	95
III.3.1.4.4.	Comunicación .....	95
III.3.1.4.5.	Información documentada .....	97
III.3.2.	<i>Hacer</i> .....	98
III.3.2.1.	<i>Operación</i> .....	98
III.3.2.1.1.	Planificación y control operacional .....	98
III.3.2.1.2.	Evaluación de riesgos de seguridad de la información.....	98
III.3.2.1.3.	Tratamiento de riesgos de seguridad de la información .....	99
III.4.	Objetivo 4. Evaluar el desempeño de la seguridad de información de la empresa CBC .....	99
III.4.1.	<i>Verificar</i> .....	99
III.4.1.1.	<i>Evaluación del desempeño</i> .....	99
III.4.1.1.1.	Monitoreo, medición, análisis y evaluación.....	99
III.4.1.1.2.	Auditoría interna .....	100
III.4.1.1.3.	Revisión por la gerencia .....	101
III.4.2.	<i>Actuar</i> .....	101
III.4.2.1.	<i>Mejora</i> .....	101
III.4.2.1.1.	No conformidades y acción correctiva .....	101
III.4.2.1.2.	Mejora continua .....	102
III.5.	O5: Verificar el cumplimiento de la implementación de la ISO 27001:2013. ....	103
<b>IV.</b>	<b>CAPÍTULO. DISCUSIÓN Y CONCLUSIONES .....</b>	<b>104</b>
IV.1.	Alcance .....	104
IV.2.	Limitaciones .....	104
IV.3.	Interpretación comparativa .....	104
<b>V.</b>	<b>REFERENCIAS.....</b>	<b>112</b>
<b>VI.</b>	<b>ANEXOS.....</b>	<b>117</b>

VI.1.	ANEXO 1. Matriz de consistencia .....	117
VI.2.	ANEXO 2. Lista de Verificación .....	118
VI.3.	ANEXO 3. Diagrama Gantt.....	124
VI.4.	ANEXO 3. Diagrama Gantt.....	125
VI.5.	ANEXO 3. Diagrama Gantt.....	126
VI.6.	ANEXO 4. Lista de verificación de expertos.....	128
VI.7.	ANEXO 5. Lista maestra.....	131
VI.8.	ANEXO 6. Aplicabilidad .....	134
VI.9.	ANEXO 7. FOR.002 Objetivos e indicadores .....	140
VI.10.	ANEXO 8. POL.008 Caracterización de procesos .....	141
VI.11.	ANEXO 9. FOR.003 Programa anual del SIG.....	143
VI.12.	ANEXO 10. Acta de Comité .....	145
VI.13.	ANEXO 11. Políticas de seguridad de la información .....	146
VI.14.	ANEXO 12. MOF .....	151
VI.15.	ANEXO 13. Rendición de cuentas .....	155
VI.16.	ANEXO 14. Alcance .....	156
VI.17.	ANEXO 15. Procedimiento de Gestión de riesgos y oportunidades .....	157
VI.18.	ANEXO 16. Procedimiento de Gestión de activos .....	158
VI.19.	ANEXO 17. Procedimiento de Gestión de riesgos SI .....	159
VI.20.	ANEXO 18. Procedimiento de G.RRHH .....	160
VI.21.	ANEXO 19. FOR.018 Evaluación del desempeño .....	161
VI.22.	ANEXO 20. PRO.008 Capacitación.....	162
VI.23.	ANEXO 21. Comunicaciones .....	163
VI.24.	ANEXO 22. PRO.001 Control de información documentada.....	169
VI.25.	ANEXO 23. PRO.004 Gestión de cambio.....	170
VI.26.	ANEXO 24. PRO.015 Infraestructura Tecnológica.....	171
VI.27.	ANEXO 25. PRO.003 Gestión de auditoría .....	172
VI.28.	ANEXO 26. FOR.009 Programa anual de auditoría.....	173
VI.29.	ANEXO 27. PRO.011 Gestión de Proveedores .....	174
	ANEXO 28. PRO.007 Revisión por la direcció .....	175
VI.30.	ANEXO 29. PRO.002 Tratamiento de NC y acción correctiva .....	176
VI.31.	ANEXO 30. FOR.007 Registro de Acciones correctiva .....	177
VI.32.	ANEXO 30. Verificación de Controles SI.....	178

## ÍNDICE DE TABLAS

<b>Tabla 1</b> Organizaciones Internacionales certificadas con la ISO 27001:2013 .....	13
<b>Tabla 2</b> Organizaciones nacionales certificadas con la ISO 27001:2013 .....	16
<b>Tabla 3</b> Técnicas, instrumentos y herramientas de recolección y análisis de datos .....	40
<b>Tabla 4</b> Procedimiento .....	41
<b>Tabla 5</b> Calificación del Check list .....	45
<b>Tabla 6</b> Cumplimiento de la norma ISO 27001:2013 antes de la implementación .....	46
<b>Tabla 7</b> Costos de RRHH .....	47
<b>Tabla 8</b> Costo Total según su tipo .....	48
<b>Tabla 9</b> Beneficio .....	49
<b>Tabla 10</b> Costo/beneficio .....	49
<b>Tabla 11</b> Partes interesadas y requisitos .....	53
<b>Tabla 12</b> Valoración de activo .....	62
<b>Tabla 13</b> Inventario de Activos .....	63
<b>Tabla 14</b> Inventario de Activos .....	64
<b>Tabla 15</b> Inventario de Activos .....	65
<b>Tabla 16</b> Inventario de Activos .....	66
<b>Tabla 17</b> Inventario de Activos .....	67
<b>Tabla 18</b> Inventario de Activos .....	68
<b>Tabla 19</b> Valor del activo .....	69
<b>Tabla 20</b> Probabilidad del riesgo .....	70
<b>Tabla 21</b> Impacto del riesgo .....	71
<b>Tabla 22</b> Matriz de riesgo .....	74
<b>Tabla 23</b> Matriz de riesgo .....	75
<b>Tabla 24</b> Matriz de riesgo .....	76
<b>Tabla 25</b> Matriz de riesgo .....	77
<b>Tabla 26</b> Matriz de riesgo .....	78
<b>Tabla 27</b> Matriz de riesgo .....	79
<b>Tabla 28</b> Matriz de riesgo .....	80
<b>Tabla 29</b> Matriz de riesgo .....	81
<b>Tabla 30</b> Matriz de riesgo .....	82
<b>Tabla 31</b> Tratamiento SI .....	84
<b>Tabla 32</b> Objetivos .....	93
<b>Tabla 33</b> Cumplimiento de la implementación .....	103

## ÍNDICE DE FIGURAS

<b>Figura 1</b> Certificación de la ISO 27001:2013.....	13
<b>Figura 2</b> Denuncias recibidas en la DIVINDAT (2015-abril 2021) .....	15
<b>Figura 3</b> Denuncias recibidas en la DIVINDAT de enero a abril 2021 .....	15
<b>Figura 4</b> Certificación ISO 27001:2013 .....	16
<b>Figura 5</b> Foda .....	52
<b>Figura 6</b> Mapa de proceso.....	54
<b>Figura 7</b> Política de excelencia organizacional.....	57
<b>Figura 8</b> Organigrama .....	58
<b>Figura 9</b> Nivel de riesgo .....	72
<b>Figura 10</b> Formato de Plan anual de capacitaciones .....	95
<b>Figura 11</b> Programa de comunicaciones y sensibilización interna.....	96
<b>Figura 12</b> Lista de Verificación .....	118
<b>Figura 13</b> Diagrama de Gantt .....	124
<b>Figura 14</b> Lista de verificación de expertos .....	128
<b>Figura 15</b> Lista maestra .....	131
<b>Figura 16</b> Aplicabilidad.....	134
<b>Figura 17</b> Objetivos e indicadores de CBC.....	140
<b>Figura 18</b> Caracterización de procesos .....	141
<b>Figura 19</b> Programa anual 2021.....	143
<b>Figura 20</b> Acta de Comité.....	145
<b>Figura 21</b> Políticas de Seguridad de la Información .....	146
<b>Figura 22</b> <i>Manual de organización y funciones</i> .....	151
<b>Figura 23</b> Rendición de cuentas.....	155
<b>Figura 24</b> Alcance.....	156
<b>Figura 25</b> Procedimiento de Gestión de riesgos y oportunidades .....	157
<b>Figura 26</b> Procedimiento de Gestión de Activos .....	158
<b>Figura 27</b> Gestión de riesgos operacionales de SI .....	159
<b>Figura 28</b> Gestión de RRHH .....	160
<b>Figura 29</b> Evaluación del desempeño.....	161
<b>Figura 30</b> Procedimiento de Capacitación .....	162
<b>Figura 31</b> Comunicaciones SI .....	163
<b>Figura 32</b> Procedimiento de Control de información documentada .....	169
<b>Figura 33</b> Procedimiento de Gestión de Cambio .....	170
<b>Figura 34</b> Procedimiento Infraestructura Tecnológica .....	171
<b>Figura 35</b> Procedimiento de Gestión de Auditoría .....	172
<b>Figura 36</b> Programa de auditoría 27001:2013 .....	173
<b>Figura 37</b> Gestión de proveedores .....	174
<b>Figura 38</b> Revisión por la dirección .....	175
<b>Figura 39</b> Tratamiento de NC y AC.....	176
<b>Figura 40</b> Registro de AC .....	177
<b>Figura 41</b> Controles SI .....	178

## RESUMEN

La presente investigación tiene como objetivo general implementar el sistema de gestión de seguridad de la información basado en la ISO 27001:2013 en la empresa Core Business Corp. SAC para proteger la información en los procesos Operativos. Asimismo, se hizo uso de las técnicas de observación y revisión documentada, el instrumento usado fue la lista de verificación para comprobar el cumplimiento de la norma ISO 27001:2013 y matriz de consistencia, además, se usaron las herramientas de diagrama Gantt y matriz de riesgos con la finalidad de dar respuesta a los objetivos de la presente investigación. La metodología usada fue el ciclo PHVA y MAGERIT permitiendo lograr la implementación. Como resultado, se obtuvo en el diagnóstico organizacional un 38 % de cumplimiento, desarrollándose la implementación de la norma ISO 27001:2013, culminando así con un 100%. Además, al costo/beneficio fue de 1.96, siendo el beneficio mayor al costo y por ende la implementación es rentable para Core Business. En conclusión, la implementación permite proteger los activos de información mediante los controles definidos al realizar el análisis de riesgos de SI dentro del capítulo 6.1.3 de la norma ISO 27001:2013, además de contar con beneficios que permiten dar cumpliendo con los objetivos de la presente investigación.

**Palabras clave:** Norma ISO 27001:2013, cumplimiento, lista de verificación, matriz de riesgos, activos de información.



## ABSTRACT

The general objective of this is to implement the information security management system based on ISO 27001: 2013 in the company Core Business Corp. SAC to protect information in Operational processes, thus we respond to the problem. Likewise, observation and documented review techniques were used, the instrument used was the checklist to verify compliance with the ISO 27001: 2013 standard and consistency matrix, in addition, the Gantt chart and matrix tools were used. risks in order to respond to the objectives of this research. Likewise, the PHVA and MAGERIT metodología is used, allowing implementation to be achieved. As a result, 38% compliance was obtained in the organizational diagnosis, developing the implementation of the ISO 27001: 2013 standard, thus culminating with 100%. In addition, the cost / benefit was 1.96, the benefit being greater than the cost and therefore the implementation is profitable for Core Business. In conclusion, the implementation allows the protection of information assets through the controls defined when carrying out the IS risk analysis within chapter 6.1.3 of the ISO 27001: 2013 standard, in addition to having benefits that allow us to comply with the objectives of the present investigation.

**Keywords:** ISO 27001: 2013 Standard, compliance, checklist, risk matrix, information assets.

## **NOTA DE ACCESO**

**No se puede acceder al texto completo pues contiene datos confidenciales**

## V. REFERENCIAS

- Benites Durand, C. A. (2019). Implementación de un sistema de gestión de seguridad de la información. *in* Aguilera Díaz, A. (2017). El costo-beneficio como herramienta de decisión en la inversión en actividades científicas. *Cofin Habana*, 11(2), 322-343.
- America Economía. (2014). *La fuga de información es una de las razones por las que las empresas pierden más dinero*. <https://mba.americaeconomia.com/articulos/notas/la-fuga-de-informacion-es-una-de-las-razones-por-las-que-las-empresas-pierden-mas-di>
- Dirección General de Modernización Administrativa. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. [file:///C:/Users/Lucero/Desktop/CORE%20BUSSINES/SI/Documentos/2012\\_Magerit\\_v3\\_libro1\\_metodo\\_es\\_NIPO\\_630-12-171-8.pdf](file:///C:/Users/Lucero/Desktop/CORE%20BUSSINES/SI/Documentos/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf)
- Fonquernie González, A. (2015, diciembre 8). *La información en las empresas*. <https://blogs.deusto.es/master-informatica/la-informacion-en-las-empresas/>
- Giesecke Sara Lafosse, M. P., & Giesecke Sara Lafosse, M. P. (2020). Elaboración y pertinencia de la matriz de consistencia cualitativa para las investigaciones en ciencias sociales. *Desde el Sur*, 12(2), 397-417. <https://doi.org/10.21142/des-1202-2020-0023>
- Iso Tools, E. (2017). *¿Cuáles son los pasos a seguir para obtener la certificación ISO 27001?* <https://www.isotools.pe/cuales-los-pasos-seguir-obtener-la-certificacion-iso-27001/>

Isotools Excellence. (s. f.-a). *¿En qué consiste una matriz de riesgos?* Recuperado 9 de noviembre de 2021, de <https://www.isotools.org/2015/08/06/en-que-consiste-una-matriz-de-riesgos/>

Isotools Excellence. (s. f.-b). *¿Qué es un checklist y como se debe utilizar?* Recuperado 9 de noviembre de 2021, de <https://www.isotools.org/2018/03/08/que-es-un-checklist-y-como-se-debe-utilizar/>

Medina León, A., Ricardo Alonso, A., Piloto Fleitas, N., Nogueira Rivera, D., Hernández Nariño, A., & Cuétara Sánchez, L. (2014). Índices integrales para el control de gestión: Consideraciones y fundamentación teórica. *Ingeniería Industrial*, 35(1), 94-104.

NIÑO MORANTE, N. R. (2018). *MODELO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN – SGSI, PARA FORTALECER LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y MONITOREAR LOS ACTIVOS DE INFORMACIÓN PARA EL INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA - INEI FILIAL LAMBAYEQUE*.  
<http://repositorio.unprg.edu.pe:8080/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%C3%91O%20MORANTE.pdf?sequence=1&isAllowed=y>

Norton. (2012). *13º Congreso sobre Prevención del Delito y Justicia Penal, Doha, del 12 al 19 de abril de 2015*.  
<https://www.un.org/es/events/crimecongress2015/cibercrime.shtml>

OBS. (s. f.). *¿Qué es un diagrama de Gantt y para qué sirve?* OBS Business School. Recuperado 9 de noviembre de 2021, de <https://www.obsbusiness.school/blog/que-es-un-diagrama-de-gantt-y-para-que-sirve>

- Torres Navarro, C., & Callegari Malta, N. (2016). Criterios para cuantificar costos y beneficios en proyectos de mejora de calidad. *Ingeniería Industrial*, 37(2), 151-163.
- formación—Norma ISO 27001 para la fábrica Radiadores Fortaleza. *Universidad Tecnológica del Perú*. <http://repositorio.utp.edu.pe/handle/20.500.12867/1933>
- Córdoba Perdomo, J. F. (2021). *Diseño de un sistema automatizado de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales en el departamento de sistemas de una institución universitaria en Colombia*. <https://repositorio.upeu.edu.pe/handle/20.500.12840/4789>
- Gascón, M. (2021, octubre 13). *Espionaje industrial: Cuando el objetivo de los malos es infiltrarse en los recovecos cibernéticos de las empresas*. 20bits. <https://www.20minutos.es/tecnologia/ciberseguridad/espionaje-industrial-cuando-el-objetivo-de-los-malos-es-infiltrarse-en-los-recovecos-ciberneticos-de-las-empresas-4852775/>
- Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2014). *Metodología de la Investigación 6ta Edición*. <https://librosenpdf.org/metodologia-de-la-investigacion-sampieri/>
- Jan, E. (s. f.). *13º Congreso sobre Prevención del Delito y Justicia Penal, Doha, del 12 al 19 de abril de 2015*. Recuperado 21 de octubre de 2021, de <https://www.un.org/es/events/crimecongress2015/cibercrime.shtml>
- JAVIER, J. (2008). *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo.

- Llanos, S., & Elías, 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*. 83.
- Pae. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*.  
[https://administracionelectronica.gob.es/pae\\_Home#.YXdhUZ7MLIU](https://administracionelectronica.gob.es/pae_Home#.YXdhUZ7MLIU)
- Torres Chango, C. D. (2020). *Plan de seguridad informática basado en la norma iso 27001, para proteger la información y activos de la empresa privada Megaprofer S.A.*  
<https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30690>
- Valdeolmillos, C. (2021, octubre 15). *Más de la mitad de empresas pierden datos por no hacer copias de seguridad suficientes*. MuyComputerPRO.  
<https://www.muycomputerpro.com/2021/10/15/empresas-pierden-datos-copias-seguridad>
- Vásquez Escalante, J. F. (2018). Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI. *Universidad Nacional Mayor de San Marcos*. <https://cybertesis.unmsm.edu.pe/handle/20.500.12672/8436>
- Vilca Mosquera, E. C. (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. *Universidad de Huánuco*.  
<http://localhost:8080/xmlui/handle/123456789/809>
- Yagual del Valle, C., & Rodriguez, L. (2014). *Análisis para la integración de un Sistema de Gestión de Seguridad de la Información(SGSi) ISO 21002 Utilizando OSSIM para una empresa industrial*. 155.