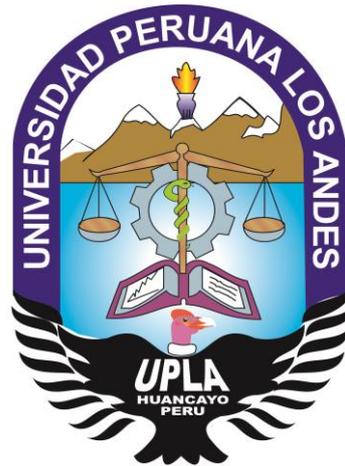


# **UNIVERSIDAD PERUANA LOS ANDES**

## **FACULTAD DE INGENIERÍA**

### **ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN**



### **INFORME TECNICO**

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA  
INFORMACIÓN BASADO EN LA ISO/IEC 27001:2014  
EN UN ESTABLECIMIENTO DE SALUD**

PRESENTADO POR:

Bach. CESAR AUGUSTO BROCCA CASTILLO

PARA OPTAR EL TITULO PROFESIONAL DE  
INGENIERO DE SISTEMAS Y COMPUTACION

**Huancayo - Perú**

**2019**

## HOJA DE CONFORMIDAD DE JURADOS

---

Dr. Casio Aurelio Torres López  
Presidente

---

Dr. Magno Teófilo Baldeón Tovar  
Jurado Revisor

---

Ing. Rafael Edwin Gordillo Flores  
Jurado Revisor

---

Ing. Jessica Vílchez Gutarra  
Jurado Revisor

---

Mg. Miguel Ángel Carlos Canales  
Secretario Docente

## **DEDICATORIA Y AGRADECIMIENTO**

Dedico este trabajo a mi querida Madre, con la mayor gratitud y admiración por los esfuerzos realizados para ayudarme a concretar mi carrera profesional; asimismo hago un reconocimiento muy especial a mis Profesores por sus enseñanzas y a mis Docentes Revisores, Jessica Gutarra, Rafael Gordillo, Magno Baldeòn. Por su apoyo incondicional.

# INDICE

INDICE DE CUADROS .....	vi
INDICE DE FIGURAS .....	ix
RESUMEN .....	xiv
ABSTRACT .....	xv
INTRODUCCIÓN .....	xvi
CAPÍTULO I.....	18
PLANTEAMIENTO DEL PROBLEMA .....	18
1.1 Problema.....	19
1.1.1 Problema General.....	19
1.1.2 Problemas específicos .....	19
1.2 Objetivos.....	20
1.2.1 Objetivo general .....	20
1.2.2 Objetivos específicos.....	20
1.3 Justificación.....	20
1.3.1 Práctica o Social.....	20
1.3.2 Metodológica .....	21
1.4 Delimitación .....	21
1.4.1 Espacial .....	21
1.4.2 Temporal.....	22
1.4.3 Económica .....	22
CAPÍTULO II.....	23
MARCO TEÓRICO .....	23
2.1 Antecedentes.....	23
2.1.1 Nacionales.....	23
2.1.2 Internacionales .....	24
2.2 Marco conceptual .....	26
2.2.1 Términos y definiciones .....	27
CAPÍTULO III.....	33
METODOLOGÍA .....	33
3.1 Tipo de estudio .....	33
3.2 Nivel de estudio.....	33
3.3 Diseño de estudio.....	33

3.3.1	Población y Muestra.....	30
3.4.	Técnicas e Instrumentos de Recolección de Datos y Análisis de Datos.....	30
<b>CAPÍTULO IV .....</b>		<b>32</b>
<b>DESARROLLO DEL INFORME.....</b>		<b>32</b>
4.1	Resultados.....	32
4.2	Discusión de los resultados .....	116
<b>CONCLUSIONES .....</b>		<b>118</b>
<b>RECOMENDACIONES .....</b>		<b>119</b>
<b>REFERENCIAS BIBLIOGRÁFICAS .....</b>		<b>120</b>
<b>ANEXOS.....</b>		<b>122</b>

## INDICE DE CUADROS

Cuadro N°.4.1. Validación de la muestra de Pre y Pos Test.....	32
Cuadro N°.4.2. Análisis del Pre Test - 1. "¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?" .....	33
Cuadro N°.4.3. Análisis del Pos Test - 1. "¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?" .....	33
Cuadro N°.4.4. Comparación del Pre y Pos Test - 1. "¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?" .....	34
Cuadro N°.4.5. Análisis del Pre Test - 2. "¿Su computadora recibe mantenimiento de manera periódica?" .....	35
Cuadro N°.4.6. Análisis del Pos Test - "¿Su computadora recibe mantenimiento de manera periódica?" .....	36
Cuadro N°.4.7. Comparación del Pre y Pos Test - 2. "¿Su computadora recibe mantenimiento de manera periódica?" .....	37
Cuadro N°.4.8. Pre Test - 3. "¿Realiza copias de información de su labor diaria?".	38
Cuadro N°.4.9. Pos Test - 3. "¿Realiza copias de información de su labor diaria?"	39
Cuadro N°.4.10. Comparación del Pre y Pos Test - 3. "¿Realiza copias de información de su labor diaria?" .....	40
Cuadro N°.4.11. Pre Test - 4. "¿Utiliza mecanismo de cifrado para su memoria USB?" .....	41
Cuadro N°.4.12. Post Test - 4. "¿Utiliza mecanismo de cifrado para su memoria USB?" .....	42
Cuadro N°.4.13. Comparación del Pre y Pos Test - 4. "¿Utiliza mecanismo de cifrado para su memoria USB?" .....	43
Cuadro N°.4.14. Pre Test - 5. "¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora?" .....	44
Cuadro N°.4.15. Post Test - 5. "¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora?" .....	45
Cuadro N°.4.16. Comparación del Pre y Pos Test - 5. "¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora.....	47
Cuadro N°.4.17. Pre Test - 6. "¿Tiene conocimiento sobre el plan de inventario de equipos?" .....	48
Cuadro N°.4.18. Pos Test - 6. "¿Tiene conocimiento sobre el plan de inventario de equipos?" .....	48

Cuadro N°.4.19. Comparación del Pre y Pos Test - 6. "¿Tiene conocimiento sobre el plan de inventario de equipos?" .....	50
Cuadro N°.4.20. Pre Test - 7. "¿Tiene conocimiento sobre el control registros de incidentes?" .....	51
Cuadro N°.4.21. Post Test - 7. "¿Tiene conocimiento sobre el control registros de incidentes?" .....	51
Cuadro N°.4.22. Comparación del Pre y Pos Test - 7. "¿Tiene conocimiento sobre el control registros de incidentes?" .....	53
Cuadro N°.4.23. Pre Test - 8. "¿Tiene conocimiento sobre el control de préstamos de equipos?" .....	54
Cuadro N°.4.24. Post Test - 8. "¿Tiene conocimiento sobre el control de préstamos de equipos?" .....	55
Cuadro N°.4.25. Comparación del Pre y Pos Test - 8. "¿Tiene conocimiento sobre el control de préstamos de equipos?" .....	56
Cuadro N°.4.26. Pre Test - 9. "¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?" .....	57
Cuadro N°.4.27. Pos Test - 9. "¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?" .....	58
Cuadro N°.4.28. Comparación del Pre y Pos Test - - 9. "¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?" .....	59
Cuadro N°.4.29. Pre Test - 10. "¿Ud. apaga o bloquea su computadora cuando se va almorzar?" .....	60
Cuadro N°.4.30. Post Test - 10. "¿Ud. apaga o bloquea su computadora cuando se va almorzar?" .....	60
Cuadro N°.4.31. Comparación del Pre y Pos Test - 10. "¿Ud. apaga o bloquea su computadora cuando se va almorzar?" .....	62
Cuadro N°.4.32. Pre Test - 11. "¿Con que frecuencia cambia su contraseña del equipo?" .....	63
Cuadro N°.4.33. Pos Test - 11. "¿Con que frecuencia cambia su contraseña del equipo?" .....	64
Cuadro N°.4.34. Comparación del Pre y Pos Test - 11. "¿Con que frecuencia cambia su contraseña del equipo?" .....	65
Cuadro N°.4.35. Pre Test - 12. "¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?" .....	66

Cuadro Nº.4.36. Pos Test - 12. "¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?" .....	67
Cuadro Nº.4.37. Comparación del Pre y Pos Test - 12. "¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?" .....	68
Cuadro Nº.4.38. Pre Test - 13. "¿Tiene alguna restricción para ingresar a los servicios de Internet?" .....	69
Cuadro Nº.4.39. Pos Test - 13. "¿Tiene alguna restricción para ingresar a los servicios de Internet?" .....	69
Cuadro Nº.4.40. Comparación del Pre y Pos Test - 13. "¿Tiene alguna restricción para ingresar a los servicios de Internet?" .....	70
Cuadro Nº.4.41.Pre Test - 14. "¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?" .....	71
Cuadro Nº.4.42. Pos Test - 14. "¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?" .....	72
Cuadro Nº.4.43. Comparación del Pre y Pos Test - 14. "¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?" .....	74
Cuadro Nº.4.44.Pre Test - 15. "¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información del establecimiento de salud?" .....	75
Cuadro Nº.4.45.Pos Test - 15. "¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información del establecimiento de salud?" .....	76
Cuadro Nº.4.46.Comparación del Pre y Pos Test- 15. "¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información del establecimiento de salud?" .....	77
Cuadro Nº.4.47. Conocimiento sobre seguridad de la información.....	78
Cuadro Nº.4.48. Participación en charlas de capacitación .....	79
Cuadro Nº.4.49. Personal sin acuerdo de confidencialidad. ....	80
Cuadro Nº.4.50.Personal con acuerdo de confidencialidad. ....	81
Cuadro Nº.4.51. Incidentes que afectan la seguridad de los datos. ....	83
Cuadro Nº.4.52. Reducción de incidentes. ....	85
Cuadro Nº.4.53. Comité de gestión de seguridad de la información. ....	87
Cuadro Nº.4.54. Comité operativo de seguridad de la información. ....	88

Cuadro N°.4 55.Inventario de activos.....	95
Cuadro N°.4 56.Tasación de activos.....	99
Cuadro N°.4 57.Análisis del riesgo.....	101
Cuadro N°.4 58.Evaluación de riesgos.....	105
Cuadro N°.4 59.Tratamiento de riesgos.....	108

## INDICE DE FIGURAS

Figura 4. 1. Análisis del Pre Test - 1. "¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?" .....	33
Figura 4. 2. Análisis del Pos Test - 1. "¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?" .....	34
Figura 4. 3. Análisis del Pre y Pos Test - "Las políticas de Seguridad de Información que se aplican en su área de trabajo" .....	35
Figura 4. 4. Análisis del Pre Test - "Recibe mantenimiento de manera periódica la computadora" .....	35
Figura 4. 5. Análisis del Pos Test - "Recibe mantenimiento de manera periódica la computadora" .....	36
Figura 4. 6. Análisis del Pre y Pos Test "Recibe mantenimiento de manera periódica la computadora" .....	38
Figura 4. 7. Análisis del Pre Test - 3. "¿Realiza copias de información de su labor diaria?" .....	39
Figura 4. 8. Análisis del Pre y Pos Test 3. "¿Realiza copias de información de su labor diaria?" .....	40
Figura 4. 9. Análisis de comparación del Pre y Pos Test - 3. "¿Realiza copias de información de su labor diaria?" .....	41
Figura 4. 10.Análisis del Pre Test - 4. "¿Utiliza mecanismo de cifrado para su memoria USB?" .....	42
Figura 4. 11. Análisis del Pos Test - 4. "¿Utiliza mecanismo de cifrado para su memoria USB?" .....	43
Figura 4. 12. Análisis de Comparación del Pre y Pos Test Test - 4. "¿Utiliza mecanismo de cifrado para su memoria USB?" .....	44
Figura 4. 13. Análisis del Pre Test - 5. "¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora?" .....	45

Figura 4. 14. Análisis del Pos Test - 5. "¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora?" .....	46
Figura 4. 15. Análisis de Comparación del Pre y Pos Test - 5. "¿Qué mecanismo de control de acceso se aplica al momento de ingresar a la computadora.....	47
Figura 4. 16. Análisis del Pre Test - 6. "¿Tiene conocimiento sobre el plan de inventario de equipos?" .....	48
Figura 4. 17. Análisis del Pos Test - 6. "¿Tiene conocimiento sobre el plan de inventario de equipos?" .....	49
Figura 4. 18. Análisis de comparación del Pre y Pos Test - 6. "¿Tiene conocimiento sobre el plan de inventario de equipos?" .....	50
Figura 4. 19. Análisis del Pre Test - 7. "¿Tiene conocimiento sobre el control registros de incidentes?" .....	51
Figura 4. 20. Análisis del Pos Test - 7. "¿Tiene conocimiento sobre el control registros de incidentes?" .....	52
Figura 4. 21. Análisis de comparación del Pre y Pos Test - 7. "¿Tiene conocimiento sobre el control registros de incidentes?" .....	53
Figura 4. 22. Análisis del Pre Test - 8. "¿Tiene conocimiento sobre el control de préstamos de equipos?" .....	54
Figura 4. 23. Análisis del Pos Test - 8. "¿Tiene conocimiento sobre el control de préstamos de equipos?" .....	55
Figura 4. 24. Análisis de comparación del Pre y Pos Test - 8. "¿Tiene conocimiento sobre el control de préstamos de equipos?" .....	56
Figura 4. 25. Análisis del Pos Test - 9. "¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?" .....	57
Figura 4. 26. Análisis del Pos Test - 9. "¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?" .....	58
Figura 4. 27. Análisis de comparación del Pre y Pos Test - - 9. "¿En caso de daño de su computadora, que tiempo se demoran en arreglarlo?" .....	59
Figura 4. 28. Análisis del Pre Test - 10. "¿Ud. apaga o bloquea su computadora cuando se va almorzar?" .....	60
Figura 4. 29. Análisis del Pos Test - 10. "¿Ud. apaga o bloquea su computadora cuando se va almorzar?" .....	61
Figura 4. 30. Análisis de comparación del Pre y Pos Test - 10. "¿Ud. apaga o bloquea su computadora cuando se va almorzar?" .....	62

Figura 4. 31. Análisis del Pre Test - 11. "¿Con que frecuencia cambia su contraseña del equipo?" .....	63
Figura 4. 32. Análisis del Pos Test - 11. "¿Con que frecuencia cambia su contraseña del equipo?" .....	64
Figura 4. 33. Análisis de comparación del Pre y Pos Test - 11. "¿Con que frecuencia cambia su contraseña del equipo?" .....	65
Figura 4. 34. Análisis del Pre Test - 12. "¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?" .....	66
Figura 4. 35. Análisis del Pos Test - 12. "¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?" .....	67
Figura 4. 36. Análisis de comparación del Pre y Pos Test - 12. "¿Utiliza la misma contraseña para todos los servicios que usa en Internet (Facebook, Correo, etc.)?" .....	68
Figura 4. 37. Análisis del Pre Test - 13. "¿Tiene alguna restricción para ingresar a los servicios de Internet?" .....	69
Figura 4. 38. Análisis del Pos Test - 13. "¿Tiene alguna restricción para ingresar a los servicios de Internet?" .....	70
Figura 4. 39. Análisis de comparación del Pre y Pos Test - 13. "¿Tiene alguna restricción para ingresar a los servicios de Internet?" .....	71
Figura 4. 40. Análisis del Pre Test - 14. "¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?" .....	72
Figura 4. 41. Análisis del Pos Test - 14. "¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?" .....	73
Figura 4. 42. Análisis de comparación del Pre y Pos Test - 14. "¿Qué mecanismo de control se aplica al momento de acceder a recursos compartidos en la red?" ....	74
Figura 4. 43. Análisis del Pre Test - 15. "¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información del establecimiento de salud?" .....	75
Figura 4. 44. Análisis del Pos Test - 15. "¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información del establecimiento de salud?" .....	76
Figura 4. 45. Análisis de comparación del Pre y Pos Test- 15. "¿Se lleva algún registro de los acontecimientos riesgosos en cuanto al uso de los equipos y de la información del Establecimiento de Salud?" .....	77
Figura 4. 46. Conocimiento sobre seguridad de la información.....	79
Figura 4. 47. Participación en charlas de capacitación .....	79

Figura 4. 48.cláusula de Confidencialidad y No divulgación de la información en los términos de referencia (TDR) .....	82
Figura 4. 49.Reducción de incidentes.....	85

## INDICE DE TABLAS

Tabla 1. Escala de Likert.....	129
Tabla 2. Probabilidad de la ocurrencia de la amenaza .....	130
Tabla 3. Evaluación del Riesgo .....	131
Tabla 4. Nivel del riesgo.....	132
Tabla 5. Estimación del Nivel del Riesgo.....	133

## RESUMEN

El presente Informe Técnico tuvo como problema general: ¿Cómo influye la implementación del Sistema de Gestión de Seguridad de la Información basado en los requisitos de la Norma Técnica Peruana ISO/IEC 27001:2014 en los niveles de riesgo de los establecimientos de salud? el objetivo general fue: Determinar cómo influye la implementación del Sistema de Gestión de Seguridad de la Información basado en los requisitos de la Norma Técnica Peruana ISO/IEC 27001:2014 reduce los niveles de riesgo de los establecimientos de salud.

En este informe es un estudio de tipo aplicado, de nivel descriptivo y de diseño pre-experimental. La población estuvo conformado por los trabajadores del Centro de Salud Alicia Lastre de la Torre del Distrito de Barranco de la ciudad de Lima, el tipo de muestreo fue el no probabilístico y la muestra estuvo dirigida a los 33 trabajadores que hacen uso de la información de las historias clínicas.

La conclusión principal de este estudio fue que la implementación del Sistema de Gestión de Seguridad de la Información basado en los requisitos de la Norma Técnica Peruana ISO/IEC 27001:2014 se ha reducido los niveles de riesgo, dado que durante el procesamiento del instrumento de trabajo se obtuvo una mejora sustancial en relación a la seguridad de los datos de los pacientes que manejan los establecimientos de salud de la Dirección de Redes Integradas de Salud Lima Sur.

**Palabras claves:** Sistema de Gestión de Seguridad de la Información, Norma Técnica Peruana ISO/IEC 27001:2014, Control de riesgo.

## **ABSTRACT**

The present Technical Report had as a general problem: How does the implementation of the Information Security Management System based on the requirements of the Peruvian Technical Standard ISO / IEC 27001: 2014 influence the risk levels of health facilities? The general objective was to: Determine how the implementation of the Information Security Management System based on the requirements of the Peruvian Technical Standard ISO / IEC 27001: 2014 influences the risk levels of health facilities.

In this report it is an applied type study, descriptive level and pre-experimental design. The population was made up of the workers of the Alicia Lastre de la Torre Health Center in the District of Barranco in the city of Lima, the type of sampling was non-probabilistic and the sample was addressed to the 33 workers who make use of the information on The medical records

The main conclusion of this study was that the implementation of the Information Security Management System based on the requirements of the Peruvian Technical Standard ISO / IEC 27001: 2014 has reduced risk levels, given that during the processing of the instrument The work obtained a substantial improvement in relation to the data security of the patients who manage the health facilities of the Directorate of Integrated Health Networks Lima Sur.

Keywords: Information Security Management System, Peruvian Technical Standard ISO / IEC 27001: 2014, risk control.

## INTRODUCCIÓN

La información en estos tiempos es considerada como una parte muy importante de toda organización y por lo tanto se debe asegurar contra la ocurrencia de cualquier incidente ocasionado por el hombre o por la naturaleza y para esto el Estado Peruano por intermedio de INDECOPI, publico en el año 2014, la Norma Técnica Peruana ISO/IEC 27001:2014 y que de acuerdo a la Resolución Ministerial N°. 004-2016-PCM, publicada en el año 2016, aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

Las entidades que prestan servicios de salud tienen las herramientas necesarias para la lograr obtener niveles aceptables de seguridad, basado en la NTP ISO/IEC 27001:2014.

Los Establecimientos de Salud de la Dirección de Redes Integradas de Salud Lima Sur, recopila y custodia datos de miles de pacientes, cuya información constituye datos sensibles, por tanto estos deben preservar de tal manera que se asegure la Confidencialidad, Integridad y Disponibilidad de los datos de la Historia Clínica, evitando la sustracción, divulgación de datos de los pacientes, teniendo en cuenta que muchas veces dañan la imagen de la institución, así como también funcionarios y trabajadores se ven inmersos en asuntos legales y administrativos.

Este informe para su mejor presentación tiene la siguiente estructura capitular:

Capítulo I: Planteamiento del Problema, en este capítulo identificamos los problemas, objetivos, justificación y la delimitación espacial, temporal y económica del informe.

Capítulo II: Marco Teórico, el presente capítulo contiene los antecedentes nacionales e internacionales, el marco conceptual y la definición de términos.

Capítulo III: Metodología, contiene el tipo de estudio, nivel de estudio y diseño de estudio, población y muestra, técnica e instrumentos de recolección y análisis de datos.

Capítulo IV: Desarrollo del Informe

Este capítulo contiene los resultados, las actividades desarrolladas en las etapas de Planificación, Implementación, Revisión y Mejora que conforman el Sistema de Gestión de la Seguridad de la Información, así como también la discusión de los resultados.

Finalmente se presentan las conclusiones, referencias bibliográficas, recomendaciones y los anexos.

Bach. Cesar Augusto Brocca Castillo