

FACULTAD DE INGENIERÍA



Carrera de Ingeniería de Sistemas Computacionales

“IMPLEMENTACIÓN DE CONTROLES SEGÚN LA
NTP-ISO/IEC 27001:2014 EN LA GESTIÓN DE
ACCESOS DE LA EMPRESA SECURITAS SAC EN
LIMA 2021”

Tesis para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autores:

Yonathan Damner Montenegro Martinez

Christian Augusto Conislla Ramirez

Asesor:

Mg. Ing. Jorge Alfredo Guevara Jiménez

Lima - Perú

2021

TABLA DE CONTENIDOS

DEDICATORIA	2
AGRADECIMIENTO	3
ÍNDICE DE TABLAS	6
ÍNDICE DE FIGURAS	7
RESUMEN	8
ABSTRACT	9
CAPÍTULO I. INTRODUCCIÓN	10
1.1. BASES TEÓRICAS.....	10
1.1.1. Bases teóricas de variable para Controles de Acceso.....	10
1.1.1.1. Definición de controles de acceso	10
1.1.1.2. NTP-ISO/IEC 27001	11
1.1.1.3. Familia de normas ISO 27001	14
1.1.1.4. Seguridad de la información	15
1.1.1.5. Análisis de cumplimiento (GAP)	15
1.1.1.6. Modelo de madurez (COBIT)	16
1.1.1.7. Análisis de riesgos	17
1.1.1.8. MAGERIT	18
1.1.1.9. Control de acceso basado en puertos	20
1.1.1.10. Okta verify	20
1.1.1.11. Manejo de identidades de acceso (IAM)	21
1.1.1.12. IDaaS (Identidad como servicio).....	21
1.1.2. Bases teóricas de variable para Gestión de Accesos.....	22
1.1.2.1. Bases teóricas de dimensión políticas de accesos a usuarios.....	23
1.1.2.2. Bases teóricas de dimensión administración de accesos a usuarios	24
1.1.2.3. Bases teóricas de responsabilidades de usuario	26
1.1.2.4. Bases teóricas de accesos a sistemas y aplicativos	27
1.2. ANTECEDENTES.....	28
1.2.1. Antecedentes internacionales	28
1.2.2. Antecedentes nacionales.....	30
1.2.3. Antecedentes locales.....	34
1.3. REALIDAD PROBLEMÁTICA.....	36
1.3.1. Información de la Empresa	36
1.4. FORMULACIÓN DEL PROBLEMA	41
1.4.1. Problema General	41
1.4.2. Problema específico	41
1.5. OBJETIVOS	41
1.5.1. Objetivo general	41
1.5.2. Objetivo específico	42
1.6. HIPÓTESIS	42
1.6.1. Hipótesis general.....	42
1.6.2. Hipótesis específica.....	42
1.7. JUSTIFICACIÓN	43
1.8. OPERACIONALIZACIÓN DE VARIABLES	44
CAPÍTULO II. MÉTODO	47
2.1. MÉTODOS Y ANÁLISIS	47
2.1.1. Tipo de investigación.....	47
2.1.2. Diseño de la investigación.....	47
2.1.3. Método de la investigación.....	48
2.1.4. Población.....	48
2.1.5. Muestra.....	49
2.1.5.1. Muestreo	50
2.1.5.2. Muestreo no Probabilístico	50

2.1.6.	<i>Técnicas de recolección de datos e instrumentos</i>	50
2.1.6.1.	Indicadores-----	50
2.1.6.2.	Instrumentos de recolección de datos -----	52
2.1.7.	<i>Procedimiento</i>	65
2.1.8.	<i>Validez y confiabilidad del instrumento</i>	65
2.1.8.1.	Validez -----	65
2.1.8.2.	Confiabilidad -----	66
2.2.	PLAN DE IMPLEMENTACIÓN	71
2.2.1.	<i>Metodología de análisis de riesgos</i>	73
2.2.1.1.	Identificar activos -----	73
2.2.1.2.	Valoración de los activos -----	74
2.2.1.3.	Identificar amenazas -----	74
2.2.1.4.	Valoración del impacto-----	75
2.2.1.5.	Valoración de probabilidad -----	75
2.2.1.6.	Valoración de riesgos-----	76
2.2.2.	<i>Análisis GAP (Análisis de brecha)</i>	79
2.2.2.1.	Análisis de la situación actual -----	79
2.2.2.2.	Establecer el estado deseado-----	83
2.2.2.3.	Analizar de deficiencias -----	83
2.2.3.	<i>Plan de trabajo de implementación</i>	85
2.2.3.1.	Análisis de la situación-----	85
2.2.3.2.	Recursos-----	91
2.2.3.3.	Funciones y responsabilidades -----	91
2.2.3.4.	Método de implementación-----	92
2.2.3.5.	Actividades de implementación-----	93
2.2.4.	<i>Aspectos éticos</i>	111
CAPÍTULO III. RESULTADOS		112
3.1.	ANÁLISIS DESCRIPTIVO	112
3.1.1.	<i>Análisis de resultados comparativos del pre-test y post-test totales</i>	112
3.1.2.	<i>Análisis de resultados comparativos del pre-test y post-test para la dimensión políticas de acceso a usuarios (D1)</i>	113
3.1.3.	<i>Análisis de resultados comparativos del pre-test y post-test para la dimensión administración de acceso a usuarios (D2)</i>	115
3.1.4.	<i>Análisis de resultados comparativos del pre-test y post-test para la dimensión responsabilidad a usuarios (D3)</i>	116
3.1.5.	<i>Análisis de resultados comparativos del pre-test y post-test para la dimensión acceso a sistemas y aplicaciones (D4)</i>	118
3.2.	ANÁLISIS INFERENCIAL	119
3.2.1.	<i>Pruebas de normalidad</i>	119
3.2.2.	<i>Pruebas de hipótesis</i>	121
3.2.2.1.	Pruebas de hipótesis específica HE1 -----	121
3.2.2.2.	Pruebas de hipótesis específica HE2 -----	122
3.2.2.3.	Pruebas de hipótesis específica HE3 -----	123
3.2.2.4.	Pruebas de hipótesis específica HE4 -----	124
CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES		125
4.1.	DISCUSIÓN	125
4.2.	LIMITACIONES	127
4.3.	RECOMENDACIONES.....	128
4.4.	CONCLUSIONES	128
REFERENCIAS		131
ANEXOS		136

ÍNDICE DE TABLAS

TABLA 1. LISTA DE CONTROLES DE ACCESO SEGÚN NTP-ISO/IEC 27001:2014	12
TABLA 2. LISTA DE SISTEMAS DE INFORMACIÓN CONSIDERADOS COMO ACTIVOS	39
TABLA 3. OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE	45
TABLA 4. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE	46
TABLA 5. MUESTRA DE SISTEMAS DE INFORMACIÓN SECURITAS SAC	49
TABLA 6. RESUMEN DE RESULTADOS DE VALORACIÓN DE EXPERTOS	66
TABLA 7. TABLA DE VALORES DE CORRELACIÓN DE PEARSON Y SU INTERPRETACIÓN	68
TABLA 8. CORRELACIONES TEST/RETEST POLÍTICAS DE ACCESO (D1)	68
TABLA 9. CORRELACIONES TEST/RETEST ADMINISTRACIÓN DE ACCESO A USUARIOS (D2)	69
TABLA 10. CORRELACIONES TEST/RETEST RESPONSABILIDAD A USUARIOS (D3)	70
TABLA 11. CORRELACIONES TEST/RETEST ACCESO A SISTEMAS Y APLICACIONES (D4)	70
TABLA 12. ESTIMACIÓN DE IMPACTO ADAPTADO DE MAGERIT V3	75
TABLA 13. ESTIMACIÓN DE PROBABILIDAD ADAPTADO DE MAGERIT V3	75
TABLA 14. PREGUNTAS RELACIONADAS A PROCEDIMIENTOS DE CONTROLES DE ACCESO.	79
TABLA 15. TABLA DE VALORACIÓN DE PROCEDIMIENTOS	80
TABLA 16. RESULTADOS DE GRADO DE CUMPLIMIENTO POR DIMENSIÓN.	81
TABLA 17. TABLA DE VALORACIÓN Y NIVEL DE MADUREZ	83
TABLA 18. RIEGOS Y CONTROLES IDENTIFICADOS PARA SU MITIGACIÓN	86
TABLA 19. LISTA DE CONTROLES A IMPLEMENTAR Y SU REFERENCIA A LA NORMA Y DIMENSIÓN	88
TABLA 20. TABLA DE APLICACIÓN DE CONTROLES SEGÚN RIEGOS Y CONTROLES	92
TABLA 21. TABLA DE APLICACIÓN DE CONTROLES SEGÚN EL SISTEMA DE INFORMACIÓN	93
TABLA 22. DESCRIPCIÓN DE PROCESOS PARA CICLO DE VIDA DE IDENTIDADES	100
TABLA 23 COMPARATIVO EN FUNCIONALIDADES DE SAAS IAM	108
TABLA 24. RESULTADOS PRE POST GRADO CUMPLIMIENTO POLÍTICAS DE ACCESOS.	114
TABLA 25. ESTADÍSTICOS DESCRIPTIVOS PRE POST DE POLÍTICAS DE ACCESO A USUARIO	115
TABLA 26. RESULTADOS PRE POST GRADO CUMPLIMIENTO ADMINISTRACIÓN DE ACCESO A USUARIOS	116
TABLA 27. ESTADÍSTICOS DESCRIPTIVOS PRE POST DE ADMINISTRACIÓN DE ACCESO A USUARIOS.	116
TABLA 28. RESULTADOS PRE POST GRADO CUMPLIMIENTO DE RESPONSABILIDAD DE ACCESO A USUARIOS.	117
TABLA 29. ESTADÍSTICOS DESCRIPTIVOS PRE POST DE RESPONSABILIDAD DE ACCESO A USUARIOS.	118
TABLA 30. RESULTADOS PRE POST GRADO CUMPLIMIENTO DE ACCESO A SISTEMAS Y APLICACIONES	119
TABLA 31. ESTADÍSTICOS DESCRIPTIVOS PRE POST DE ACCESO A SISTEMAS Y APLICACIONES.	119
TABLA 32. PRUEBAS DE NORMALIDAD DE DIMENSIONES PRE Y POST	120
TABLA 33. PRUEBA T-STUDENT PARA POLÍTICAS DE ACCESO A USUARIOS.	121
TABLA 34. PRUEBA T-STUDENT PARA ADMINISTRACIÓN DE ACCESO A USUARIOS	122
TABLA 35. PRUEBA T-STUDENT PARA RESPONSABILIDAD DE ACCESO A USUARIOS.	123
TABLA 36. PRUEBA T-STUDENT PARA ACCESO A SISTEMAS Y APLICACIONES.	124

ÍNDICE DE FIGURAS

FIGURA 1. DOMINIOS DE LA NORMA ISO 27001.....	11
FIGURA 2. FAMILIA ISO 27000.	14
FIGURA 3. ETAPAS ANÁLISIS GAP.	16
FIGURA 4. NIVELES DE CAPACIDAD PARA LOS PROCESOS. FUENTE: COBIT 2019 INTRODUCCIÓN Y METODOLOGÍA.....	17
FIGURA 5. ELEMENTOS DE ANÁLISIS DE RIESGO POTENCIALES.	19
FIGURA 6. PROCESO DE GESTIÓN DE ACCESOS POR ITIL.	23
FIGURA 7. TAMAÑOS DE MERCADO PARA SERVICIOS DE SEGURIDAD 2020.....	37
FIGURA 8. INFRACCIONES DE DATOS Y HACKEOS DE DATOS MÁS GRANDES DEL MUNDO (2015-2021).	38
FIGURA 9. FICHA DE REGISTRO DE DATOS – PRE TEST – POLÍTICAS DE ACCESO A USUARIO.....	53
FIGURA 10. FICHA DE REGISTRO DE DATOS – PRE TEST – ADMINISTRACIÓN DE ACCESO A USUARIOS.	54
FIGURA 11. FICHA DE REGISTRO DE DATOS – PRE TEST – RESPONSABILIDAD DE ACCESO A USUARIOS.....	55
FIGURA 12. FICHA DE REGISTRO DE DATOS – PRE TEST – ACCESO A SISTEMAS Y APLICACIONES.	56
FIGURA 13. FICHA DE REGISTRO DE DATOS – RE TEST – POLÍTICAS DE ACCESO A USUARIO.....	57
FIGURA 14. FICHA DE REGISTRO DE DATOS – RE TEST – ADMINISTRACIÓN DE ACCESO A USUARIOS	58
FIGURA 15. FICHA DE REGISTRO DE DATOS – RE TEST – RESPONSABILIDAD DE ACCESO A USUARIOS.....	59
FIGURA 16. FICHA DE REGISTRO DE DATOS – RE TEST – ACCESO A SISTEMAS Y APLICACIONES.....	60
FIGURA 17. FICHA DE REGISTRO DE DATOS – POST TEST – POLÍTICAS DE ACCESO A USUARIO.	61
FIGURA 18. FICHA DE REGISTRO DE DATOS – POST TEST – ADMINISTRACIÓN DE ACCESO A USUARIOS.....	62
FIGURA 19. FICHA DE REGISTRO DE DATOS – POST TEST – RESPONSABILIDAD DE ACCESO A USUARIOS.	63
FIGURA 20. FICHA DE REGISTRO DE DATOS – POST TEST – ACCESO A SISTEMAS Y APLICACIONES.	64
FIGURA 21. DIAGRAMA DE PROCESOS DE IMPLEMENTACIÓN.....	72
FIGURA 22. CRITERIOS DE ACEPTACIÓN DEL RIESGO.	76
FIGURA 23. MATRIZ DE RIESGOS ADAPTADO DE MAGERIT V3.	77
FIGURA 24. UMBRALES DE RIESGO ADAPTADO DE MAGERIT V3.	77
FIGURA 25. RESULTADOS DE VALORACIÓN DE RIESGOS, ACCIONES Y PRIORIDADES	78
FIGURA 26. GRADO DE CUMPLIMIENTO POR DIMENSIÓN (PRE).....	82
FIGURA 27. RESULTADOS DE ANÁLISIS DE BRECHAS (PRE)	82
FIGURA 28. ANÁLISIS GAP ESTADO ACTUAL VS OBTENIDO.	84
FIGURA 29. PROCESO ANTERIOR DE GESTIÓN DE ACCESOS.	94
FIGURA 30. PROCESO IMPLEMENTADO PARA LA GESTIÓN DE ACCESOS.	95
FIGURA 31. ESQUEMA DE RED SECURITAS CON PROTOCOLO 802.1X.	96
FIGURA 32. MODELO DE RED BASADO EN PROTOCOLO IEEE 802.1X.	97
FIGURA 33. PROCESO DE CICLO DE VIDA DE IDENTIDADES	99
FIGURA 34. PROCESO GENERAL DE MANEJO DE CUENTAS PRIVILEGIADAS IMPLEMENTADO.....	102
FIGURA 35 CUADRANTE MÁGICO DE GARTNER.....	108
FIGURA 35. ARQUITECTURA ACTUAL DE ACCESO DE LOS USUARIOS A LOS SISTEMAS	109
FIGURA 36. ARQUITECTURA OKTA SECURITAS PARA INICIO DE SESIÓN	109
FIGURA 37. GRADO DE CUMPLIMIENTO TOTALES (PRE VS POST).....	112
FIGURA 38. GRADO DE CUMPLIMIENTO POR DIMENSIÓN (PRE VS POST)	113
FIGURA 39. GRADO DE CUMPLIMIENTO PRE VS POST TEST PARA LA DIMENSIÓN POLÍTICAS DE ACCESO A USUARIOS.....	114
FIGURA 40. GRADO DE CUMPLIMIENTO PRE VS POST TEST PARA LA DIMENSIÓN ADMINISTRACIÓN DE ACCESO A USUARIOS.	115
FIGURA 41. GRADO DE CUMPLIMIENTO PRE VS POST TEST PARA LA DIMENSIÓN RESPONSABILIDAD DE ACCESO A USUARIOS.	117
FIGURA 42. GRADO DE CUMPLIMIENTO PRE VS POST TEST PARA LA DIMENSIÓN ACCESO A SISTEMAS Y APLICACIONES.	118

RESUMEN

La siguiente tesis “Implementación de controles según la NTP-ISO/IEC 27001:2014 en la gestión de accesos de la empresa SECURITAS SAC en Lima 2021” tiene como objetivo definir e implementar los controles de acceso para la empresa SECURITAS SAC, se efectuó un análisis de brechas (GAP) para conocer el estado de cumplimiento en el uso de controles de acceso y el estado deseado, asimismo se realizó un análisis de riesgo encontrando las probabilidades que existen en la materialización de un posible ataque y el impacto. Esto se realizó tomando como base la Norma NTP-ISO/IEC 27001:2014, enfocada en el Anexo A9 – Control de Accesos. Esto debido a que SECURITAS SAC ha presentado casos que han afectado a las operaciones debido al no tener implementado correctamente una buena gestión de accesos en el área de administración de TI. La tesis menciona los conceptos teóricos y su metodología para el desarrollo de la misma. Se uso el muestreo no probabilístico y por conveniencia, utilizando herramientas de observación y registro en fichas con la validación de juicio de expertos para la muestra de 10 sistemas tomadas en distintos tiempos (Pre-test, Re-Test y Post-Test) con un enfoque cuantitativo. Se pudo observar que el nivel de grado de cumplimiento inicial está por debajo de lo necesario por lo cual la implementación logra incrementar el grado de madurez de controles a un nivel aceptable por la empresa a un estado “Gestionado” que representa a más del 75% dando como valido y funcional la implementación.

Palabras clave: Controles de acceso, Gestión de accesos, Análisis de Riesgo, Seguridad de la Información, Normas ISO, Políticas de Acceso.

ABSTRACT

The following thesis "Implementation of controls according to the NTP-ISO / IEC 27001: 2014 in access management of the company SECURITAS SAC in Lima 2021" aims to define and implement access controls for the company SECURITAS SAC, a Gap analysis to know the state of compliance in the use of access controls and the desired state, a risk analysis was also carried out, finding the probabilities that exist in the materialization of a possible attack and the impact. This was done based on the NTP-ISO / IEC 27001: 2014 Standard, focused on Annex A9 - Access Control. This is due to the fact that SECURITAS SAC has presented cases that have affected operations due to not having correctly implemented good access management in the IT administration area. The thesis mentions the theoretical concepts and its methodology for its development. Non-probability and convenience sampling was used, using observation and recording tools in cards with the validation of expert judgment for the sample of 10 systems taken at different times (Pre-test, Re-Test and Post-Test) with a quantitative approach. It was observed that the initial level of compliance is below what is necessary, so the implementation manages to increase the degree of maturity of controls to an acceptable level for the company to a "Managed" state that represents more than 75% giving the implementation as valid and functional.

Keywords: Access Control, Access Management, Risk Analysis, Information Security, ISO Standards, Access Policies.

NOTA DE ACCESO

No se puede acceder al texto completo pues contiene datos confidenciales

REFERENCIAS

- Antonucci, D. (2017). *The cyber risk handbook: Creating and measuring effective cybersecurity capabilities*. New Jersey: Wiley.
- Acosta, J. J. (2018). *Diseño para la automatización del mantenimiento de usuarios en el proceso de ceses y la reducción del riesgo de fuga de información en el Banco Financiero del Perú*. Universidad Tecnológica del Perú Lima, Perú.
- Arias, E. S. (2020). *Implementación de la norma ISO 27001 en el Departamento de Tecnología de Información de la empresa Esvicsac, Callao*. Universidad Cesar Vallejo Lima, Perú.
- Avalos, C. V. (2019). *Diseño de un modelo de control de accesos a los sistemas de información basado en la ISO 27001 en una financiera*, Universidad Norbert Wiener Lima, Perú.
- Avenía, C. (2017). *Fundamentos de seguridad informática*. Colombia, Bogotá: Fondo editorial Areandino.
- Bridget, K. (2019). *ISO 27001 Controls - a Guide to Implementing and Auditing*. United Kingdom: IT Governance Ltd.
- Caldas, J. C. (2020). *Evaluación de control de accesos en correval*. Universidad Piloto de Colombia, Bogotá, Colombia.
- Calder, A. (2017). *Nueve Pasos para El éxito: Una Visión de Conjunto para la Aplicación de la ISO 27001:2013*. Reino Unido: IT Governance Ltd.
- C. Rupa, R. Patan, F. Al-Turjman and L. Mostarda, "Enhancing the Access Privacy of IDaaS System Using SAML Protocol in Fog Computing," in *IEEE Access*, vol. 8, pp. 168793-168801, 2020, doi: 10.1109/ACCESS.2020.3022957.

- Carmona, D. H. (23 de diciembre de 2016). Aspectos esenciales para fomentar el control de acceso de la información. *Gestión Competitividad e Innovación*. P.54-59.
- Cutillas Zárata, J. (2021). Mejora al sistema de seguridad de una empresa mediante gestión de identidades (Doctoral dissertation, Universitat Politècnica de València).
- Davila, M. A. (2018). Evaluación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, en la municipalidad distrital de JOSÉ CRESPO Y CASTILLO -AUCAYACU. Universidad católica los ángeles de Chimbote, Perú.
- Delgado, M. M. & Vásquez, J. L. (2020). MODELO DE SEGURIDAD INFORMÁTICA APLICANDO LA NORMA ISO/IEC 27001 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN EN LA EMPRESA BERENDSON NATACIÓN SRL. Universidad de Lambayeque Chiclayo, Perú.
- Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT - versión 3.0*. Madrid, España: Ministerio de Hacienda y Administraciones Públicas de España.
- Escalante, D. M. (2019). Diseño de un sistema de gestión de seguridad de la información bajo el enfoque de la ntp iso/iec 27001 para la Dirección de Salud Virgen de Cocharcas–Chincheros. Universidad nacional José maría Arguedas Apurímac, Perú.
- Ferruzola, E., Duchimaza, J., Ramos, J. y Alejandro, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. *Revista Científica y Tecnológica UPSE*, 6(1), 34-41. DOI: 10.26423/rctu.v6i1.429
- Flores, K. L. & Flores, C. E. (diciembre de 2021) Pruebas para comprobar la normalidad de datos en procesos productivos. *Revista de ciencias sociales y humanísticas*. Vol. 23, No. 2, pp 83-106
- Gabriel-Ortega, J. (2017). Cómo se genera una investigación científica que luego sea motivo de publicación. *Journal of the Selva Andina Research Society*, 8(2), 155-156.

- Gabriel-Ortega, J. (2017). Cómo se genera una investigación científica que luego sea motivo de publicación. *Journal of the Selva Andina Research Society*, 8(2), 155-156.
- Galindo, H. (2020). ESTADÍSTICA PARA NO ESTADÍSTICOS UNA GUÍA BÁSICA SOBRE LA METODOLOGÍA CUANTITATIVA DE TRABAJOS ACADÉMICOS. España, Alicante: Editorial Área de Innovación y Desarrollo S.L
- Graus, E. G. (Enero de 2018). Estadística aplicada a la investigación educativa. Dilemas Contemporáneos. Recuperado de www.dilemascontemporaneoseduccionpoliticayvalores.com
- He, W & Zhang, Z (2019). Enterprise cybersecurity training and awareness programs: recommendations for success, *Journal of Organizational Computing and Electronic Commerce*, 249-257, 2019.
- Hernández, C. E. & Carpio, N. (15 de febrero de 2019) Metodología de la investigación. Revista científica de instituto nacional de Salud. Recuperado de www.alerta.salud.gob.sv
- ISACA. (2019). Marco de referencia COBIT® 2019: Introducción y Metodología, 2019. Schaumburg, IL 60173, USA. ISBN 978-1-60420-788-0.
- ITIL®4 Foundation (2019). Guía de fundamentos en castellano. United States, Seattle: Axelos
- Lalinde, J. D. H., Castro, F. E., Rodríguez, J. E., Rangel, J. G. C., Sierra, C. A. T., Torrado, M. K. A., & Pirela, V. J. B. (2018). Sobre el uso adecuado del coeficiente de correlación de Pearson: definición, propiedades y suposiciones. *Archivos venezolanos de Farmacología y Terapéutica*, 37(5), 587-595.
- Neil, D. A. & Suarez, L. C. (2018). Procesos y fundamentos de la investigación científica. Machala, Ecuador: Editorial UTMACH.

- Normaiso27001. (2019). Guía para implementar ISO 27001 paso a paso. Recuperado de <https://normaiso27001.es>
- Parra, A. M. (2017). Diagnóstico de la gestión de acceso de usuarios en la Superintendencia de Servicios públicos domiciliarios-norma ISO/IEC 27001: 2013 numerales a. 9.2. 2 y a. 9.3. 1. Universidad Libre seccional Bogotá, Colombia.
- Presidencia del Consejo de Ministros (2016). Resolución Ministerial N° 004-2016-PCM. Recuperado de <https://www.gob.pe>
- Perumbuli, S. K. (2017). An Authentication Security and Governance Frame Work for Near Field Communication in Sri Lankan Context (Doctoral dissertation).
- Salazar, C. P. & Castillo, S. G. (2018) Fundamentos básicos de estadística. ISBN: 978-9942-30-616-6
- Tola, D. F & Freire, L. C. (2015). Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001. Escuela Superior Politécnica del Litoral (ESPOL) Guayaquil, Ecuador.
- Torok, G., Day, MR, Hartman-Baker, RJ y Snavely, C. (noviembre de 2020). Iris: banca de asignación y gestión de identidades y accesos para la era de la exaescala. En SC20: Conferencia internacional de informática de alto rendimiento, redes, almacenamiento y análisis (págs. 1-11). IEEE.
- Torres, M.& Salazar, F. G. & Paz, K. (2019). Métodos de recolección de datos para una investigación. Universidad Rafael Landivar Guatemala.
- Vallois, V., Mehaoua, A. y Amziani, M. (mayo de 2021). Gestión de acceso e identidad basada en blockchain en sistemas industriales de IoT. En 2021, Simposio

Internacional IFIP / IEEE sobre Gestión Integrada de Redes (IM) (págs. 623-627).

IEEE.

Vásquez, W. A. (2020). Metodología de la investigación. Recuperado de www.usmp.edu.pe

Ventura-León, J. L., Arancibia, M., & Madrid, E. (2017). La importancia de reportar la validez y confiabilidad en los instrumentos de medición: Comentarios a Arancibia et al. *Revista médica de Chile*, 145(7), 955-956.

Villasís-Keever, M. Á., Márquez-González, H., Zurita-Cruz, J. N., Miranda-Novales, G., & Escamilla-Núñez, A. (2018). El protocolo de investigación VII. Validez y confiabilidad de las mediciones. *Revista Alergia México*, 65(4), 414-421.