UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Políticas basadas en la ISO 27001:
2013 y su influencia en la gestión de seguridad
de la información en municipalidades de Perú

Tesis para obtener el Título Profesional de Ingeniero de Sistemas

Autor:

Shonerly Bustamante Garcia

Asesor:

Mg. Immer Elías Cuellar Rodríguez

Tarapoto, abril de 2021

DECLARACIÓN JURADA DE AUTORÍA DE TESIS

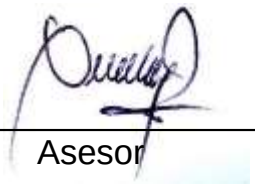
Mg. Immer Elías Cuellar Rodríguez, de la Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:

Que la presente investigación titulada: **"POLÍTICAS BASADAS EN LA ISO 27001: 2013 Y SU INFLUENCIA EN LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN MUNICIPALIDADES DE PERÚ"** constituye la memoria que presenta el Bachiller Shonerly Bustamante Garcia para obtener el título de Profesional de Ingeniero de Sistemas cuya tesis ha sido realizada en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente declaración en la ciudad de Tarapoto a los 12 días del mes de abril del año 2021.



Asesor

Mg. Immer Elías Cuellar Rodríguez

ACTA DE SUSTENTACIÓN DE TESIS

En Lima, Ñaña, Villa Unión, a.....6..... día(s) del mes de.....Abril.....del año 20.21.. siendo las...11:00 horas, se reunieron los miembros del jurado en la Universidad Peruana Unión Campus Lima, bajo la dirección del (de la) presidente(a):

……Mg. Danny Lévano Rodriguez....., el (la) secretario(a): ....Dr. Miguel Angel.....

.....Valles Coral..... y los demás miembros: ….....Mg. Marco Antonio.....

.....Ruiz Grandez ……y el (la) asesor(a) ……Mg. Immer Elias…….....

.....Cuellar Rodriguez..... con el propósito de administrar el acto académico de sustentación de la tesis titulado:

……Políticas basadas en la ISO 27001:2013 y su influencia en la gestión de seguridad de la Información en municipalidades de Perú.……..……..

…… del(los) bachiller/es: a) ….Shonerly Bustamante García.....

……b)……..……..

…… c)……..……..

……conducente a la obtención del título profesional de: ……

……Ingeniero de Sistemas……..

(Denominación del Título Profesional)

El Presidente inició el acto académico de sustentación invitando al (a la) / a (los) (las) candidato(a)/s hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del jurado a efectuar las preguntas, y aclaraciones pertinentes, las cuales fueron absueltas por al (a la) / a (los) (las) candidato(a)/s. Luego, se produjo un receso para las deliberaciones y la emisión del dictamen del jurado.

Posteriormente, el jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Bachiller-(a): ….Shonerly Bustamante García……

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	**20**	**A+**	**Excelente**	Excelencia

Bachiller -(b): ……

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	

Bachiller -(c): ……

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	

(*) Ver parte posterior

Finalmente, el Presidente del jurado invitó al (a la) / a (los) (las) candidato(a)/s a ponerse de pie, para recibir la evaluación final y concluir el acto académico de sustentación procediéndose a registrar las firmas respectivas.

Presidente/a

Secretario/a

Asesor/a

Miembro

Miembro

Bachiller (a)

Bachiller (b)

Bachiller (c)

Enfoque UTE, V.12-N.2, Abr. 2021, pp. 69-79
http://ingenieria.ute.edu.ec/enfoqueute/
e-ISSN: 1390-6542

Received: 2021/01/26
Accepted: 2021/03/24
Online: 2021/03/25
Published: 2021/04/05
https://doi.org/10.29019/enfoqueute.743

Políticas basadas en la ISO 27001: 2013 y su influencia en la gestión de seguridad de la información en municipalidades de Perú

(Policies based on ISO 27001: 2013 and its influence on information security management in municipalities of Peru)

Shonerly Bustamante García[1], *Miguel Ángel Valles Coral*[2], *Immer Elías Cuellar Rodríguez*[3], *Danny Lévano Rodríguez*[4]

Resumen

La gestión de seguridad de la información dentro de una organización debe ser un proceso bien definido, ya que implica un enorme esfuerzo tanto de usuarios, jefes de área y demás servidores para conocer cómo responder ante eventos sospechosos y cómo gestionar vulnerabilidades identificadas. El objetivo de esta investigación fue mejorar la gestión de seguridad de la información en una municipalidad distrital peruana, mediante la implantación de un modelo de políticas basado en la ISO 27001:2013. Para ello, se hizo una investigación preexperimental con una muestra de 30 trabajadores a quienes se les aplicó un cuestionario para medir el grado de satisfacción con el modelo implantado. En promedio, más del 90 % de los encuestados reconoció mejoras en la municipalidad, lo que marca una gran diferencia entre el pre y postest, de 49 % a 96 %. Se concluye que el modelo de políticas de seguridad basado en tres pilares fundamentales: confidencialidad, integridad y disponibilidad mejoró la gestión de seguridad de la información, garantizando un adecuado resguardo de los datos.

Palabras clave

Gestión, información, organización, políticas, seguridad.

Abstract

Information security management within an organization must be a well-defined process, as it involves a huge effort from users, area managers and other servers to know how to respond to suspicious events and how to manage identified vulnerabilities. The objective of this research was to improve information security management in a Peruvian district municipality, through the implementation of a policy model under ISO 27001: 2013. For this, a preexperimental investigation was carried out with a sample of 30 workers, to whom a questionnaire was applied to measure the degree of satisfaction with the implanted model. On average, more than 90 % of those surveyed recognized improvements in the municipality, marking a great difference between the pre and postest, from 49 % to 96 %. It is concluded that the security policy model, based on three fundamental pillars: confidentiality, integrity, and availability, improved information security management, guaranteeing adequate data protection.

Keywords

Information, management, organization, policies, security.

1 UPeU (Universidad Peruana Unión), Tarapoto, Perú [shonerly.bustamante@upeu.edu.pe, https://orcid.org/0000-0002-8173-203X].
2 UPeU, Tarapoto, Perú [miguel.valles@upeu.edu.pe, https://orcid.org/0000-0002-8806-2892].
3 UPeU, Tarapoto, Perú [immerc@upeu.edu.pe, https://orcid.org/0000-0001-9381-4203].
4 UPeU, Tarapoto, Perú [danlev@upeu.edu.pe, https://orcid.org/0000-0002-1783-1105].

1. Introducción

Las organizaciones utilizan la tecnología como medio para procesar, almacenar y resguardar su información (Miranda et al., 2016), aún más en tiempo de pandemia; la tecnología está jugando un rol fundamental dentro del funcionamiento de sus procesos, pero que, a la vez, estos están sometidos a un elevado número de riesgos y amenazas informáticas (Martínez, 2020).

Toda organización está expuesta cada vez más a amenazas y es vulnerable a cualquier ataque informático (Caamaño y Gil, 2020); es decir, la variedad de amenazas en contra de sus activos puede causar la pérdida, manipulación o la no disponibilidad de la información (Gil y Gil, 2017). Paralelamente, pueden ocasionar cuantiosas pérdidas económicas, tal como dicen Wiley et al. (2020), el Foro Económico Mundial, en 2018, reportó que el 65 % de organizaciones australianas fueron víctimas de ataques, una de cada diez sufrió pérdidas superiores a $ 1 millón.

La mayoría de los robos o pérdidas de información en Latinoamérica recaen sobre el sector empresarial, pues Aguilar-Antonio (2019) explica que estos incidentes se deben a las insuficientes medidas de protección, lo que causa pérdidas de productividad, credibilidad, competitividad y perjuicios financieros que comprometen la continuidad de la organización.

El uso de políticas basadas en la ISO 27001 mejoran la gestión de la seguridad de la información, pues como argumentan Angulo et al. (2018), ayudan a controlar los procesos de seguridad, garantizando la confidencialidad, integridad y disponibilidad de la información. Por ejemplo, tras el diseño e implantación de un modelo de políticas en las empresas proveedoras de internet en Ecuador se mostró mejoras significativas. Por esta razón, Cueva y Alvarado (2017) señalan que las organizaciones han adoptado nuevas formas de protección de sus activos de información. Para llegar a este punto, la solución óptima se basaría en incrementar los niveles de seguridad y protección de su información, con la implantación de políticas y/o controles de seguridad (Lux, 2018).

Santana y Aspilcueta (2016) dicen que los nuevos desafíos que enfrenta todo país emergente, tal como Perú, hacen que las organizaciones se apoyen en las tecnologías de información para suplir demandas de flexibilidad e incremento de productividad, lo que genera nuevos retos y desafíos de seguridad. Por su lado, Baca (2016) considera que la utilización de políticas y buenas prácticas repercuten significativamente en la gestión de seguridad de la información; como ejemplo menciona la implantación de un modelo de gestión de seguridad en la Unidad Educativa Local de Chiclayo, donde se mejoró el nivel de seguridad tanto en confidencialidad, integridad y disponibilidad de los datos.

Las PYMES peruanas son el foco más vulnerable. En un estudio Porras et al. (2018) afirman que un 41 % poseen probabilidades mínimas para detectar ataques sofisticados. Los principales motivos de dificultad son en un 100 % las limitaciones presupuestarias, y en un 89 % la falta de recursos especializados. Poma y Vargas (2019) informaron que, en un reporte publicado por Kaspersky, en 2019, Perú se encontraba en el puesto número 40, considerado como el país más vulnerable frente a ataques cibernéticos.

En ese contexto, el problema que hemos abordado trata sobre los mecanismos deficientes que tenía la Subgerencia de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de Morales para garantizar niveles adecuados de seguridad en la información de los dispositivos de cómputo y almacenamiento. Estos mecanismos afectaban el correcto desenvolvimiento y la efectividad en sus operaciones.

Al evaluar los mecanismos de seguridad deficientes, logramos identificar causas, tales como: i) la mínima formación del personal en seguridad de la información. Moreno et al. (2020) consideran que la poca formación del personal ocasiona peligros de gran magnitud; ii) manejo inadecuado de los protocolos destinados a la protección de los dispositivos tecnológicos, lo que causa las fugas de información, así lo afirman Sánchez et al. (2017), incluso afectan la imagen y estabilidad de las organizaciones, y iii) insuficientes medidas en el proceso de instalación de activos informáticos, considerando que estos, en cualquier momento, pueden ser destruidos de manera no autorizada (Valencia et al., 2016).

Aparte de tener procedimientos de protección de la información inadecuadamente definidos, a esto se suma el incumplimiento de algunas políticas implantadas. Castillejos et al. (2016) explican que el incumplimiento de políticas conlleva a exponer información confidencial; asimismo, Tundidor et al. (2018) resaltan la importancia de implantar políticas, normas y procedimientos a fin de prevenir y disminuir los riesgos de pérdida de datos de la organización, ofreciendo información oportuna, clara y veraz.

La poca asignación de presupuesto para proteger los datos en la organización es uno de los principales obstáculos para garantizar un adecuado nivel de seguridad de la información. El limitado presupuesto impide ejecutar medidas orientadas a adoptar controles de seguridad que minimicen el riesgo en el manejo de la información (Diéguez y Cares, 2019).

Las organizaciones públicas, en general, están inmersas en un entorno de riesgos, lo que podría causar pérdidas debido a eventos originados por procesos, personas o tecnología (Crespo, 2017). Las políticas basadas en la Norma ISO 27001 disminuyen estos riesgos, e influyen significativamente en la gestión de seguridad de la información. En ese sentido, con la finalidad de comprobar esta hipótesis, realizamos esta investigación aplicando un modelo cuantitativo por conveniencia.

Nos plantemos como objetivo mejorar la gestión de seguridad de la información en la Subgerencia de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de Morales, de manera que i) se logró aumentar el nivel confianza de los trabajadores; ii) se garantizó la confidencialidad, integridad y disponibilidad de la información; y se generó la sensibilización del personal sobre la correcta manipulación y resguardo los distintos activos de información.

2. Metodología

En este estudio se empleó un diseño preexperimental y de corte cuantitativo. La población estuvo conformada por todos los trabajadores de la Municipalidad Distrital de Morales que a noviembre de 2020 era un total de 90 trabajadores. La muestra fue de 30 individuos y el muestreo se hizo mediante muestreo no probabilístico aplicando el tipo por conveniencia.

Para cumplir nuestro objetivo de implantación de políticas, el estudio se realizó en pleno acuerdo con el jefe de la Unidad de Informática y Sistemas y demás servidores públicos, quienes se comprometieron de manera responsable a cumplirlas y darles seguimiento.

Se aplicó la técnica de observación directa, mediante visitas programadas y entrevistas con los profesionales encargados de la administración del área informática y usuarios de los sistemas, para el proceso de identificación de los indicadores de gestión de seguridad de la información. Paralelamente, se revisaron los componentes y/o activos de información con los que cuenta la Municipalidad.

La información se recopiló a través de un instrumento para la seguridad de la información, este cuenta con 3 dimensiones y 15 indicadores en escala de Likert, con validez mediante el juicio de expertos igual a 4.73, en la escala del 1 a 5.

El diseño del instrumento se desarrolló con base en las afirmaciones de Valencia-Duque y Orozco-Alzate (2017). Los autores conciben la gestión de seguridad de la información de la siguiente manera: confidencialidad, integridad y disponibilidad. También se tuvo en cuenta el estudio de Peña y Anías (2019), en el que considera prioritaria la incorporación de políticas de seguridad de la información en las organizaciones; asimismo, la investigación de Aguilera et al. (2017), quienes, de manera interesante, aseguran que para garantizar niveles óptimos de seguridad de la información se depende de la implantación de un conjunto de medidas administrativas, operativas y técnicas.

Los datos fueron procesados mediante SPSS v.24, para su posterior tabulación, y obtención de gráficos y datos estadísticos. Del mismo modo, se realizó el análisis de datos y la verificación de la normalidad de los mismos, considerando que los datos tuvieron distribución normal, se aplicó la prueba estadística T de Student, ya que los censados fueron un total de 30 individuos, esto a fin de determinar el grado de variación del modelo de políticas de seguridad implantadas sobre la gestión de seguridad de la información.

3. Resultados y discusión

Políticas de seguridad de la información

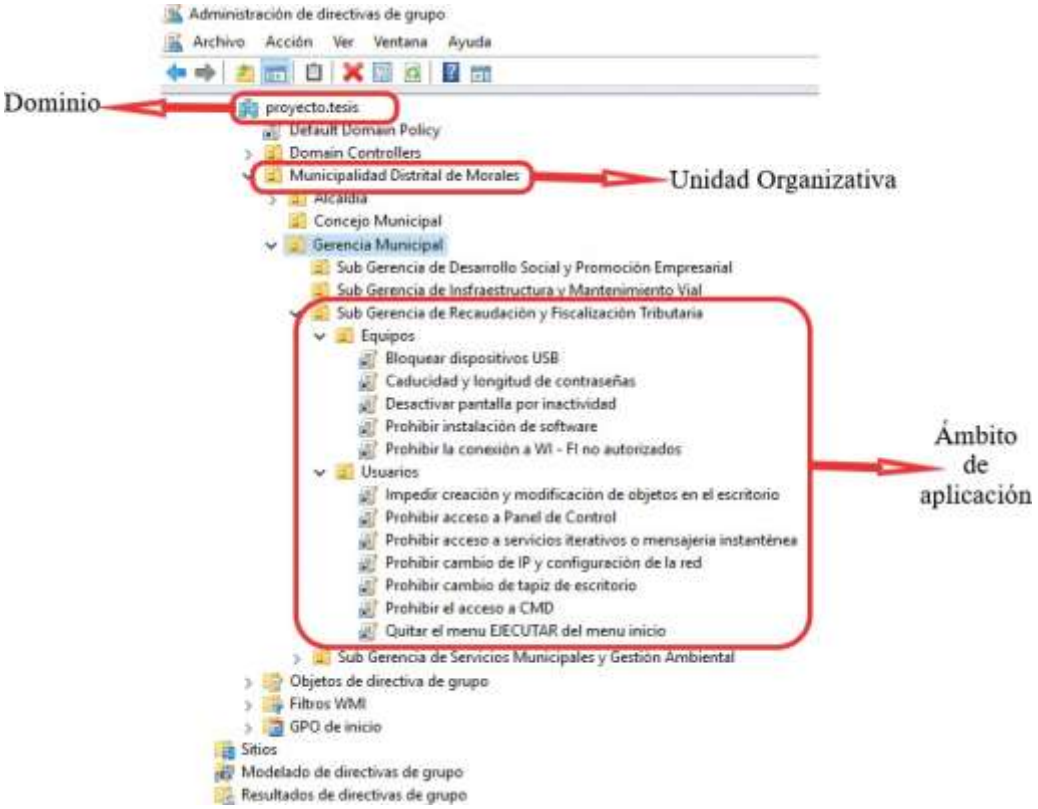
La implantación de políticas se realizó mediante la creación de directivas de grupos (los GPO), por lo que se utilizó en el sistema operativo Windows Server 2016; las directivas fueron ejecutadas bajo un entorno de virtualización, teniendo como cliente Windows 10 para así probar su funcionalidad.

Además, el óptimo funcionamiento de la propuesta, en cuanto al funcionamiento de los dispositivos de cómputo, se garantizó gracias al desarrollo de nuestro *Manual de mantenimiento preventivo de servicios tecnológicos*, además de la reubicación de algunos expuestos a amenazas naturales, conjuntamente con compromisos firmados por el jefe de la Unidad de Informática y Sistemas para garantizar su cumplimiento.

Para lograr mejor comprensión por parte del usuario, y hacer de este pieza fundamental de la gestión de seguridad, se hizo una sensibilización por áreas. Se visitó a los usuarios en sus puestos de trabajo para brindarles información de primera fuente y lograr interactuar, resolver dudas y hacer aclaraciones, a modo de hacer que ellos sean receptivo a las políticas de seguridad de la información; pues, con base en Proaño y Gavilanes (2018), es una de las estrategias fundamentales para el cumplimiento de medidas de seguridad.

La estructura de descomposición, que a continuación se ve en la Figura 1, representa la forma en que se han operado y organizado nuestras Políticas de Grupo (GPO), teniendo como dominio a proyecto.tesis y Unidad Organizativa a Municipalidad Distrital de Morales, dentro del cual se encuentra la muestra o ámbito de aplicación a la Subgerencia de Recaudación y Fiscalización Tributaria, dividida en Usuarios y Equipos, considerando que para crear cada GPO se ha mantenido un estricta inclinación hacia la ISO 27001: 2013 y, por sobre todo, los criterios utilizados se basaron en garantizar la integridad, confidencialidad y disponibilidad de la información.

Figura 1. Estructura de descomposición de GPO



Martelo et al. (2018) afirman que se debe controlar ciertas acciones para evitar ocasionar agujeros en la seguridad de la información y así controlar los flujos de entrada/salida de datos. Estas acciones son, por ejemplo, acceso a Panel de Control, a servicios iterativos o mensajería instantánea, al símbolo del sistema (CMD) y al menú EJECUTAR del menú inicio. Además, el uso de dispositivos extraíbles, la caducidad y longitud de contraseñas, e instalación no controlada de *software* puede introducir vulnerabilidades que pueden provocar fugas de información, pérdida de integridad u otros incidentes de seguridad (Hernández y Porven, 2016). Gonzáles et al. (2016) también explican que restringir conexiones a cualquier tipo de red, permite garantizar un nivel aceptable de seguridad de datos que se genera y se transmite.

Gestión de la seguridad de la información

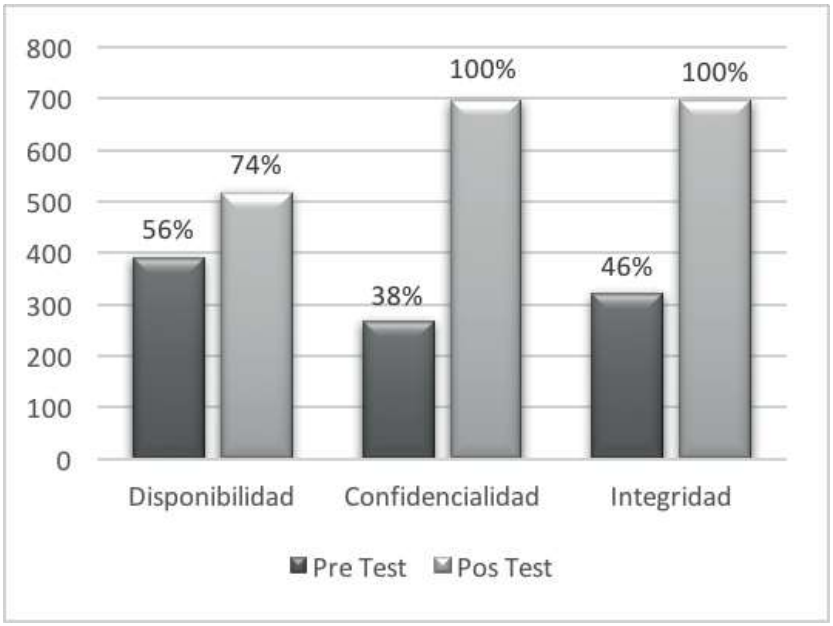
En la Tabla 1, se observa la normalidad del test, para ello se utilizó la prueba de normalidad Shapiro-Wilk, debido a que la muestra fue un total de 30 individuos. Se concluyó que los datos siguen una distribución normal, dado a que el valor de p es mayor a 0.05.

Tabla 1. Prueba de normalidad de Shapiro-Wilk

	Estadístico	gl	p
Pretest	0.945	30	0.121
Postest	0.941	30	0.099

Para evaluar la influencia de las políticas sobre la gestión de seguridad de la información, se consideraron tres pilares o dimensiones fundamentales: la disponibilidad, confidencialidad e integridad, a fin de garantizar un adecuado resguardo de los datos.

Figura 2. Gestión de seguridad de la información a nivel de dimensiones



Se aprecia que, en general, existe un resultado favorable luego de implantar las políticas de seguridad, porque, en promedio, más del 90 % de los encuestados reconoció las mejoras exitosas en la municipalidad. Se debe considerar que el análisis de los datos se hizo mediante prueba estadística t de student, tal como se muestra en la Tabla 2.

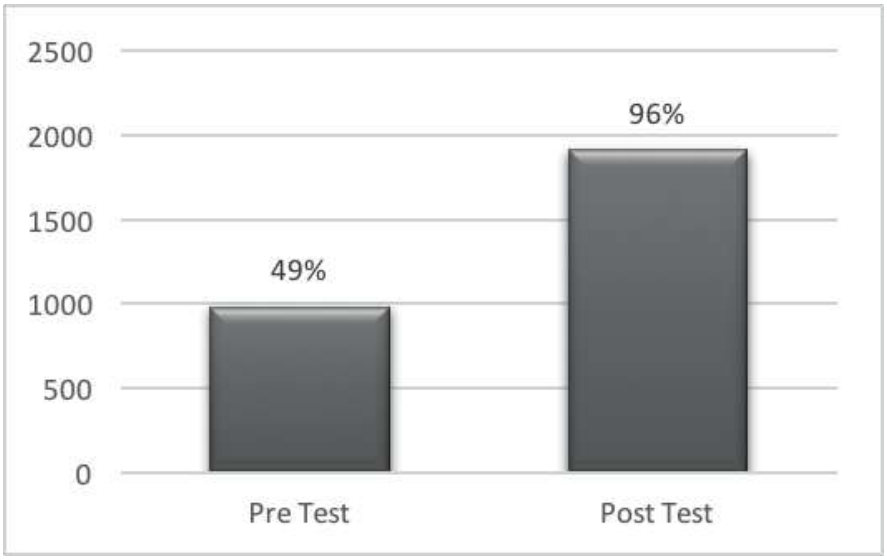
Tabla 2. Prueba t por cada dimensión del pre y postest

Dimensión	Test	t	gl	p
Disponibilidad	Pre-Post	-30.224	29	0.000
Confidencialidad	Pre-Post	-42.562	29	0.000
Integridad	Pre-Post	-11.750	29	0.000

Con base en la Tabla 2, se puede decir que hay una mejor protección de la información, porque el valor que obtiene p para disponibilidad, confidencialidad e integridad es menor a 0.05, tal como señalan Angulo et al. (2018) en su investigación, así como Cordoví et al. (2019), donde p obtuvo los mismo valores en estas dimensiones luego de haber implantado un modelo de políticas.

En la Figura 2 se muestra la diferencia significativa entre el pre-test y el post-test, pues Flores-Ruiz et al. (2017) sostienen que para comprobar las mejoras en investigaciones preexperimentales, se debe obtener cierta variación entre la evaluación inicial y la evaluación final.

Figura 3. Diferencia entre el pre y post-test



Lo anterior se debe interpretar de manera muy cuidadosa, porque, en términos generales, significa que la implantación de políticas cumplió un rol fundamental mejorando el nivel de seguridad de la información, tal como en una investigación Baca (2016) llevada a cabo en Chiclayo, donde la implantación de políticas repercutió significativamente en la gestión de la información, luego de obtener una gran diferencia entre la pre y postevaluación.

Tabla 3. Prueba t del pre y post-test

	t	gl	p
Pre-Post	-54.197	29	0.000

Los datos de la Tabla 3 permiten corroborar que se ha cumplido con nuestro objetivo planteado, porque las políticas de seguridad implantadas mejoraron la gestión de seguridad de la información dentro de la Subgerencia de Recaudación y Fiscalización Tributaria. Esto se debe eventualmente a que el valor que obtiene p es menor a 0.05, por lo cual se presenta el Modelo de políticas a partir de una visión estratégica y teniendo en cuenta las teorías de Szczepaniuk et al. (2020) y Gibert, et al. (2020).

Modelo de políticas de Seguridad de la Información según ISO 27001: 2013

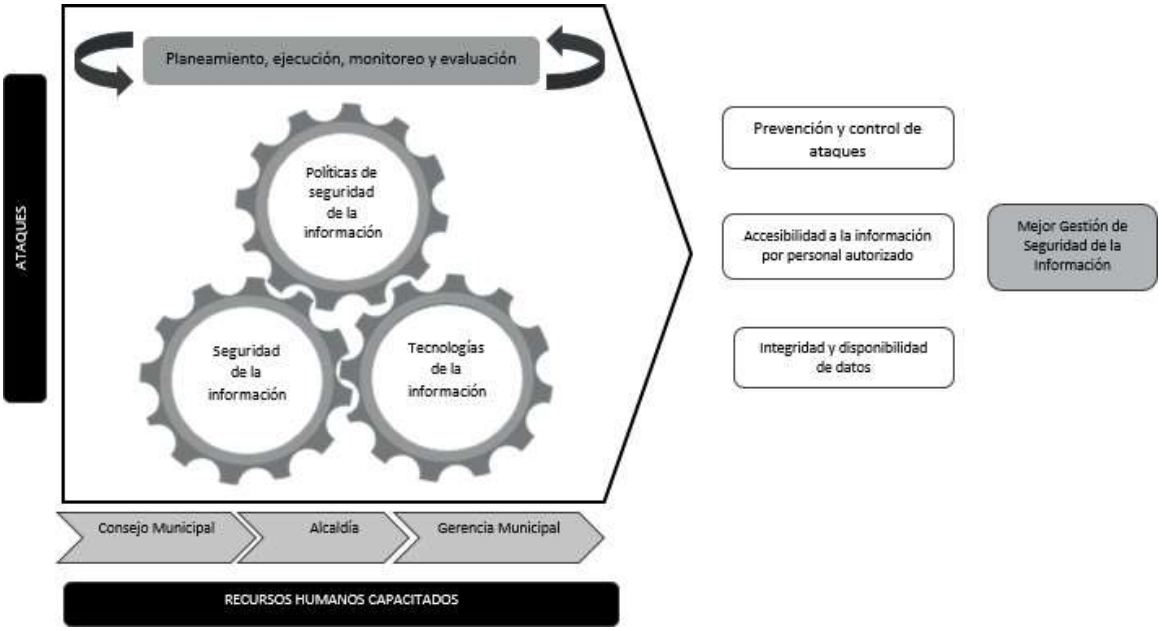
La Municipalidad Distrital de Morales tiene una enorme responsabilidad de brindar a sus ciudadanos una atención de calidad, donde la información que se maneje y que se requiera esté siempre a su alcance. Esta tarea está íntimamente ligada a la protección de la información, puesto que las organizaciones de hoy están tratando de encontrar nuevas formas de abordar adecuadamente las cuestiones de seguridad (Gil y Gil, 2017).

En ese sentido, Paananen et al. (2020) manifiestan la necesidad de implantar políticas de seguridad de la información en toda organización, pues es uno de los mecanismos eficaces para preservar la integridad, confidencialidad y disponibilidad, para birndar confianza a las personas que se benefician de los servicios. Peña y Anías (2019) creen que la implantación de políticas de

seguridad de la información en las organizaciones trae mejoras considerables en el proceso del negocio, reduciendo costos y garantizando un adecuado resguardo de datos.

En la Figura 4 se plantea el Modelo de Políticas de Seguridad de la Información que, aplicando una visión estratégica, se cumplió con los objetivos de la municipalidad. Además, se considera que estos elementos permitieron, entre otras cosas, resguardar la información y mejorar la gestión de seguridad de la institución.

Figura 4. Modelo de Políticas de Seguridad de la Información



El modelo anterior fue creado para mejorar los deficientes mecanismos y garantizar niveles adecuados de seguridad en la información de los dispositivos de cómputo y almacenamiento, cuyas vulnerabilidades fueron detectadas en la fase diagnóstica de esta investigación. En ese sentido, la implantación de políticas para afrontar los posibles problemas de seguridad ayuda a proteger la integridad, confidencialidad y disponibilidad de la información Kaleem et al. (2016).

5. Conclusiones y recomendaciones

En función de los resultados de la prueba estadística t de Student, mostrada en la Tabla 2, se concluye que el estudio ha logrado mejorar la gestión de seguridad de la información, basándose en los tres pilares fundamentales que son i) confidencialidad, que busca garantizar que la información no sea divulgada a personas o sistemas no autorizados; ii) integridad, mantener inalterable la información ante accidentes o intentos maliciosos; y iii) disponibilidad, brindar accesibilidad a la información en el momento y en la forma en que los usuarios autorizados lo requieran.

La implantación del modelo de Políticas de Seguridad de la Información basadas en las Norma ISO 27001: 2013 se llevó a cabo de manera satisfactoria. Estas políticas se encuentran alojadas en un entorno de virtualización en Windows Server 16 y documentadas en manuales y compromisos que fueron entregados directamente al jefe de Informática y Sistemas para garantizar el cumplimiento de cada política.

Se identificaron los indicadores que repercuten directamente en la gestión de seguridad de la información; además, las políticas fueron estructuradas adecuadamente con la descomposición de las Políticas de Grupo (GPO), en dominio, Unidad Organizativa y ámbito de aplicación, tal como se muestra en la Figura 1.

En consecuencia, podemos afirmar que el Modelo de Políticas de Seguridad de la Información implantado influenció positivamente en la gestión de seguridad de la información dentro de la Subgerencia de Recaudación y Fiscalización Tributaria de la Municipalidad Distrital de Morales.

El modelo se ha diseñado de tal manera que pueda ser replicado en cualquier municipalidad por lo que, en función de los resultados auspiciosos encontrados, recomendamos su aplicación tomando en cuenta las características y realidades de las instituciones donde se pretende implantar.

Referencias

Aguilar-Antonio, J.-M. (2019). Hechos ciberfísicos: Una propuesta de análisis para ciberamenazas en las estrategias nacionales de ciberseguridad. *URVIO. Revista Latinoamericana de Estudios de Seguridad*, *4299*(25), 24–40. https://doi.org/10.17141/urvio.25.2019.4007

Aguilera, O., Pérez, E., & Rivero, R. (2017). La protección de la información: Una visión desde las entidades educativas cubanas. *Ciencias de la Información*, *48*(3), 41–47. https://www.redalyc.org/pdf/1814/181457243006.pdf

Angulo, N., Zambrano, M., García, G., & Bolaños-Burgos, F. (2018). Propuesta metodológica de seguridad de información para proveedores de servicios de internet en Ecuador. *MIKARIMIN*. *Revista Científica Multidiciplinaria*, *4*(4), 165–176. http://45.238.216.13/ojs/index.php/mikarimin/article/view/1197

Baca, V. (2016). Diseño de un sistema de gestión de seguridad de información para la unidad de gestión educativa local-Chiclayo. *Ingeniería. Ciencia, Tecnología e Innovación*, 3(1), 16. http://revistas.uss.edu.pe/index.php/ING/article/view/357/346

Caamaño, E., & Gil, R. (2020). Prevención de riesgos por ciberseguridad desde la auditoría forense: Conjugando el talento humano organizacional. *Novum*, *1*(10), 20. https://revistas.unal.edu.co/index.php/novum/article/view/84210/73652

Castillejos, B., Torres, C., & Lagunes, A. (2016). La seguridad en las competencias digitales de los *millennials*. *Apertura*, *8*(2), 54–69. http://www.scielo.org.mx/pdf/apertura/v8n2/2007-1094-apertura-8-02-00054.pdf

Cordoví, V., Pardo, M., Rodríguez, N., & López, E. (2019). La gestión de información estadística relacionada con las actividades formativas en la Universidad Virtual de Salud. *Medisan*, *23*(4), 715–727. http://www.medisan.sld.cu/index.php/san/article/view/2214/pdf

Crespo, E. (2017). Ecu@Risk, una metodología para la gestión de riesgo aplicada a las MPYMES. *Enfoque UTE*, 8(1), 107–121. https://doi.org/10.29019/enfoqueute.v8n1.140

Cueva, M., & Alvarado, D. (2017). Análisis de Certificados SSL/TLS gratuitos y su implementación como mecanismo de seguridad en servidores de aplicación. (Analysis of Free SSL/TLS Certificates and Their Implementation as Security Mechanism in Application Servers). *Enfoque UTE*, *8*(1), 14. I: https://doi.org/10.29019/enfoqueute.v8n1.128

Diéguez, M., & Cares, C. (2019). Comparación de dos enfoques cuantitativos para seleccionar controles de seguridad de la información. *RISTI. Revista Ibérica de Sistemas e Tecnologias de Informação*, 32, 16. http://www.scielo.mec.pt/pdf/rist/n32/n32a09.pdf

Flores-Ruiz, E., Miranda-Novales, M., & Villasis-Keever, M. (2017). El protocolo de investigación VI: Cómo elegir la prueba estadística adecuada. Estadística inferencial. *Rev Alerg Mex*, *64*(3), 364–370. http://www.scielo.org.mx

Gil, V., & Gil, J. (2017). Seguridad informática organizacional: Un modelo de simulación basado en dinámica de sistemas. *Scientia et Technica* Año XXII, *22*(2). https://www.redalyc.org/pdf/849/84953103011.pdf

Gonzáles, A., Beltrán, D., & Fuentes, E. (2016). Propuesta de protocolos de seguridad para la red inalámbrica local de la Universidad de Cienfuegos. *Revista Científica Universidad y Sociedad*, *8*(4), 8. http://scielo.sld.cu/pdf/rus/v8n4/rus17416.pdf

Hernández, A., & Porven, J. (2016). Procedimiento para la seguridad del proceso de despliegue de aplicaciones web. *Revista Cubana de Ciencias Informáticas*, *10*(2), 15. http://scielo.sld.cu/pdf/rcci/v10n2/rcci04216.pdf

Kaleem, M., Burnap, P., & Rana, O. (2016). Identifying Cyber Risk Hotspots: A Framework for Measuring Temporal Variance in Computer Network Risk. *Computers and Security*, 57, 16. https://doi.org/10.1016/j.cose.2015.11.003

Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis*, *24*(1), 159–206. https://scielo.conicyt.cl/pdf/iusetp/v24n1/0718-0012-iusetp-24-01-00159.pdf

Martelo, R., Tovar, L., & Maza, D. (2018). Modelo básico de seguridad lógica . Caso de Estudio: El laboratorio de redes de la Universidad de Cartagena en Colombia. *Información Tecnológica*, *29*(1), 3–10. http://dx.doi.org/10.4067/S0718-07642018000100003

Martínez, F. (2020). Ciberseguridad y Estado autonómico. *ICADE. Revista de la Facultad de Derecho*, 109, 1–19. https://doi.org/https://doi.org/10.14422/icade.i109.y2020.001

Miranda, M., Valdés, O., Pérez, I., Portelles, R., & Sánchez, R. (2016). Metodología para la implementación de la gestión automatizada de controles de seguridad informática. *Revista Cubana de Ciencias Informáticas*, *10*(2), 14–26. http://scielo.sld.cu/pdf/rcci/v10n2/rcci02216.pdf

Moreno, J., Rodriguez, C., & Leguias, I. (2020). Revisión sobre propagación de *ransomware* en sistemas operativos *Windows. I+D Tecnológico*, *16*(1), 7. https://doi.org/10.33412/idt.v16.1.2438

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the Art in Information Security Policy Development. *Computers and Security*, *88*, 1–14. https://doi.org/10.1016/j.cose.2019.101608

Peña, M., & Anías, C. (2019). Sistema para ejecutar políticas sobre infraestructuras de Tecnologías de la Información: ITpolicies execution system. *Ingeniare. Revista Chilena de Ingeniería*, *27*(3), 479-494. https://scielo.conicyt.cl

Poma, A., & Vargas, R. (2019). Problemática en ciberseguridad como protección de sistemas informáticos y redes sociales en el Perú y en el mundo. *Sciéndo*, *22*(4), 8. https://doi.org/10.17268/sciendo.2019.034

Porras, J., Pastor, S., & Alvarado, R. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista Peruana de Computación y Sistemas, 1*(1), 47–56. http://dx.doi.org/10.15381/rpcs.v1i1.14856

Proaño, R., & Gavilanes, A. (2018). Estrategia para responder a incidentes de inseguridad informática ambientado en la legalidad ecuatoriana. *Enfoque UTE*, *9*(1), 90–101. https://doi.org/10.29019/enfoqueute.v9n1.229

Sánchez, N., Pulido, B., & Camacho, J. (2017). La significativa evolución en seguridad de la información para la Policía Nacional de Colombia. *Revista Logos, Ciencia & Tecnología*, *9*(1), 7. http://www.redalyc.org/articulo.oa?id=517752178018

Santana, M., & Aspilcueta, H. (2016). Prioridades de gestión de tecnologías de información en organizaciones peruanas. *Revista Venezolana de Gerencia*, *20*(72), 684–697. https://doi.org/10.31876/revista.v20i72.20926

Szczepaniuk, E., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information Security Assessment in Public Administration. *Computers and Security*, 90, 1–11. https://doi.org/10.1016/j.cose.2019.101709

Tundidor, L., Nogueira, C., & Medina, C. (2018). Exigencias y limitaciones de los sistemas de información para el control de gestión organizacional. *Universidad y Sociedad*, *10*(1), 7. http://scielo.sld.cu/pdf/rus/v10n1/2218-3620-rus-10-01-8.pdf

Valencia-Duque, F., & Orozco-Alzate, M. (2017). Metodología para la implementación de un sistema de gestión de seguridad de información basado en la familia de normas ISO/IEC 27000. *RISTI*. *Revista Iberica de Sistemas e Tecnologias de Informacão*, 22, 16. https://doi.org/10.17013/risti.22.73–88

Valencia, F., Marulanda, C., & Trujillo, M. (2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. *Revista Gerencia Tecnológica Informática*, *15*(2015), 13. https://biblat.unam.mx

Wiley, A., McCormac, A., & Calic, D. (2020). More Than the Individual: Examining the Relationship Between Culture and Information Security Awareness. *Computers and Security*, 88, 1–8. https://doi.org/10.1016/j.cose.2019.101640