UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Auditoría basada en la Norma ISO 27001 para la mejora de los Controles de Seguridad de la Información en la Gerencia de Informática y Tecnología en una municipalidad peruana.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Ingeniero de Sistemas

AUTOR:

Limaymanta Ortiz, Max Junnior (https://orcid.org/0000-0002-0520-1317)

ASESOR:

Dr. Daza Vergaray, Alfredo (https://orcid.org/0000-0002-2259-1070)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información.

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

LIMA - PERÚ

2022

Dedicatoria

El presente trabajo de investigación lo dedico principalmente a Dios, quien es mi inspiración y me potencia para seguir cumpliendo uno de mis anhelos más profundos en el proceso.

Gracias a mis padres por su amor, sacrificio y trabajo durante estos años; también que gracias a ustedes por permitir que esté aquí y de lo que soy hoy. Es un orgullo y un honor ser su hijo, son los mejores padres.

Gracias a mi hermano por estar siempre ahí y darme su apoyo moral en este periodo de mi vida. Gracias a mis tíos y tías por sus oraciones, consejos y palabras de aliento que me han hecho mejor persona y me han acompañado de alguna manera a alcanzar todos mis sueños y metas. En general gracias a toda mi familia

Gracias a todos los que me han apoyado y hecho que mi trabajo sea un éxito, especialmente a los que me han abierto puertas y compartido sus conocimientos.

Agradecimiento

En primer lugar, me gustaría agradecer a mi mentor, el Dr. Daza Vergaray Alfredo, quien me guio en cada etapa de este proyecto con su conocimiento y apoyo para lograr el resultado deseado.

También quiero agradecer a la Universidad César Vallejo y a la Municipalidad de Chorrillos por brindarme todos los recursos y herramientas que necesité para llevar a cabo el proceso de investigación. No hubiera podido lograr estos resultados sin su ayuda incondicional.

Finalmente, me gustaría agradecer a todos mis colegas y mi familia por apoyarme incluso cuando estaba desanimado.

Índice de Contenidos

Índice de Tablas

Índice de gráficos y figuras

RESUMEN

El presente trabajo de investigación tuvo como objetivo establecer si la auditoría basada en la norma ISO 27001 mejora los controles de seguridad de la información en la Gerencia de Informática y Tecnología en una Municipalidad Peruana. Evaluando los factores de la normatividad, seguridad física de la infraestructura de TI y la cultura de ciberseguridad. La metodología de investigación fue de tipo aplicada y diseño experimental del tipo pre experimental. La muestra la conformaron los 18 servidores públicos de la Gerencia de Informática y Tecnología, los instrumentos utilizados fueron la guía de observación y el cuestionario. Los resultados obtenidos en los estados de los 3 dominios de seguridad de la información obtuvieron un efecto relevante para la mejora de los controles de seguridad de la información en la gerencia de informática y tecnología. Ya que se logró alcanzar una mejora en las políticas de la seguridad (dominio A5) de 5,56% en el estado “Repetible” y 94,44% en el estado “Definido”. Por su parte la seguridad física y ambiental (dominio A11) un 66,67% en estado “Repetible” y 33,33% en “Definido”. Y por último en la seguridad ligada a los recursos humanos (dominio A7) un 55,56% en estado “Repetible” y 44,44% en estado “Definido”. Con estos resultados se evidenció que a través de la auditoría basado en la norma ISO 27001 se mejora la generación de políticas de seguridad y su cumplimiento, mejora la seguridad física de la infraestructura de TI y mejora la cultura de ciberseguridad.

Palabras claves: Controles de seguridad, auditoria, ISO 27001, ciberseguridad.

ABSTRACT

The objective of this research work was to establish if the audit based on the ISO 27001 standard improves the information security controls in the IT and Technology Management of a Peruvian Municipality. Evaluating the factors of regulations, physical security of the IT infrastructure and cybersecurity culture. The research methodology was applied and experimental design of the pre-experimental type. The sample consisted of 18 public servants of the IT and Technology Management, the instruments used were the observation guide and the questionnaire. The results obtained in the states of the 3 information security domains obtained a relevant effect for the improvement of the information security controls in the IT and technology management. An improvement in security policies (domain A5) of 5.56% in the "Repeatable" status and 94.44% in the "Defined" status was achieved. For its part, physical and environmental security (domain A11), 66.67% in "Repeatable" status and 33.33% in "Defined" status. And finally, in safety linked to human resources (domain A7), 55.56% in "Repeatable" status and 44.44% in "Defined" status. These results showed that through the audit based on the ISO 27001 standard, the generation of security policies and their compliance is improved, the physical security of the IT infrastructure is improved and the cybersecurity culture is enhanced.

Keywords: Security controls, auditing, ISO 27001, cybersecurity.

I. INTRODUCCIÓN

Los controles de seguridad de la información se pueden encontrar en el Anexo A de la norma ISO 27001, que se enfoca en garantizar la confidencialidad, disponibilidad e integridad de la información. Los controles de seguridad son fundamentales para las instituciones públicas y privadas, ya que la seguridad de la información se ha convertido en una agenda de alta prioridad para todas las organizaciones, así mismo la información es un recurso fundamental para cualquier tarea, actividad y proceso, por lo que en la actualidad la información es considerada un recurso clave que puede asemejarse con el trabajo, el capital y se define cada vez más como una representación de poder, desafortunadamente los controles de seguridad presentan diferentes problemas.

A nivel internacional, para Paguay y Zamora (2017) la seguridad de la información más que una cuestión de TI es una cuestión que involucra al negocio en sí, y que las instituciones que quieren perdurar y sobre todo progresar deben entender la relevancia de la seguridad de la información a través de controles de seguridad. El sector público y privado deberían tener mayor conciencia en la posibilidad de robo de identidad y sobre todo su información. Ya que sus correos electrónicos, sistemas informáticos incluso sus páginas puede ser vulnerados como consecuencia a los avances de la ciberdelincuencia. Para las instituciones su mayor valor es su información y esta a su vez genera una ventaja competitiva para la misma, por ello la preocupación en la seguridad de la información.

A nivel nacional, para Monteza (2019), la sociedad digital es cada vez más compleja, y a medida que aumenta nuestra dependencia de la información y la conectividad, surge la necesidad de prepararse y desarrollar resiliencia ante la variedad de ciberataques que enfrentan las organizaciones. Quienes a su vez presentan fallas tanto técnicas como de procedimiento. Desde Perú, el 55 % de los entrevistados en la encuesta mundial sobre fraude y delitos económicos de PwC de 2018 dijo que su empresa había sufrido fraude en los últimos dos años.

Asimismo, el autor Monteza (2019) también indica que en Perú disponemos de la Normativa Técnica Peruana ISO/ 27001:2014 la cual está aprobada para uso obligatorio en todas las entidades por reglamento del ministerio N° 004-2016-PCM, que forma parte del sistema de la información nacional. Sin embargo, por el

desconocimiento de los organismos públicos sobre estos temas, no tomaron medidas necesarias para su implementación.

La entidad que da soporte a la estructura de la municipalidad de Chorrillos es la Gerencia de Informática y Tecnología, que se rige a la Gerencia Municipal. Es una organización de soporte técnico encargado de la administración de los procedimientos de la tecnología informática y e-comunicación interna; elaboración de normativas y procedimientos en cuanto a control de las operaciones y fuentes de datos de salida; seguridad de los procedimientos y conservación de los componentes de TI, a fin de una administración eficaz y salvaguardar la persistencia de los procedimientos de la institución. Sus responsabilidades se extienden a las tareas asociadas con la elaboración, ejecución, funcionamiento, sostenimiento y monitoreo de los sistemas de información, así como aportar con el apoyo técnico a los beneficiarios.

Asimismo, entre las responsabilidades más importantes de la Gerencia de Informática y Tecnología es garantizar la persistencia de la institución a través de técnicas esenciales para el aseguramiento de la información, el resguardo de la documentación, asimismo en representaciones lógicas contenidas en servicio de alojamiento web, sitios web, e-mail y programa informático que son utilizados por la organización, así como servidores, ordenadores, dispositivos de almacena información sensible, redes de comunicación de datos, y en definitiva, los utilizados por los beneficiarios.

En la actualidad, la Gerencia de Informática y Tecnología cuenta con el estado inicial de los controles de seguridad de la norma ISO 27001, por ello no cuentan con directivas que sean obligatorias para todas las áreas o unidades organizacionales de la institución. También dispone con algunas revisiones de seguridad de información, los cuales se manejan sin adherirse a los lineamientos. A continuación, vamos a mencionar los controles con los que tiene hoy por hoy la gerencia: Seguridad en los dispositivos, resguardo contra software malintencionado, copias de respaldo y la administración del aseguramiento de la red.

En el plano de la seguridad de la información existen controles, pero no poseían un mecanismo de seguimiento o respuesta para medir la implantación, lo que pone en peligro todavía más en referencia a la seguridad de la información en las organizaciones. Otro factor importante que muestra la institución es la falta de aseguramiento físico de la infraestructura de TI, se puede observar claramente los problemas que esta conlleva un claro ejemplo sería el hurto, pérdida, daños del activo de la información, así como la discontinuidad de las funciones de la organización. Es un tema muy significativo la seguridad física y ambiental ya que aumenta los riesgos de accesos no permitidos e interrupciones frente a la infraestructura de tratamiento de la información en la municipalidad.

Otro punto muy importante es la falta de una cultura de ciberseguridad en los trabajadores, y esto se debe también a la poca importancia que se le da a la problemática de seguridad de la información que causa la fuga del activo de información, el utilizar páginas y programas no autorizados. Todos estos problemas con dispositivos no autorizados se deben a que desconocen las amenazas que existen en la actualidad. Según el diario “Andina” en 2020 el Perú ocupa el segundo lugar con menos ciberseguridad en América Latina a través de un estudio realizado por parte de CompariTech y mundialmente se encuentra en el lugar 17.

Entonces nuestro problema se resuelve en la siguiente pregunta: ¿Cómo la auditoría basada en la norma ISO 27001 mejorará los controles de seguridad de la información en la Gerencia de informática y tecnología en la municipalidad de Chorrillos?

Asimismo, se plantearon los siguientes problemas específicos: ¿Cómo la auditoría basada en la norma ISO 27001 mejorará la generación de políticas de seguridad y su cumplimiento en la Gerencia de informática y tecnología en la municipalidad de Chorrillos?, ¿Cómo la auditoría basada en la norma ISO 27001 mejorará la seguridad física de la infraestructura de TI en la Gerencia de informática y tecnología en la municipalidad de Chorrillos?, ¿Cómo la auditoría basada en la norma ISO 27001 mejorará la cultura de Ciberseguridad en la Gerencia de informática y tecnología en la municipalidad de Chorrillos?

El trabajo de investigación se justifica ya que permitió la mejora de los controles de seguridad de la información a través de la norma ISO 27001 que permite el resguardo de la disponibilidad, confidencialidad y la integridad del activo de la información, así como a los sistemas que lo procesa. Permitió la mejora de la generación de políticas de seguridad y su cumplimiento a través de un documento revisado y aprobado por el encargado de la gerencia, la mejora de la seguridad física de la infraestructura de TI se pudo asegurar los dispositivos a través de afiches informativos de las políticas de seguridad, así como también con la guía para el SGSI y la mejora de la cultura de ciberseguridad dando a conocer la guía para el Sistema de Gestión de Seguridad de la Información a toda la gerencia, y afiches informativos sobre las políticas en lugares estratégicos para su conocimiento.

También esta investigación se justifica ya que los resultados ayudaron a la institución interesada y a sus autoridades a conocer la importancia de los controles de seguridad de la norma ISO 27001, asimismo aporta a la tranquilidad de las personas que estén utilizan sus servicios en esta nueva era digital.

En vista de todo lo investigado, se propuso el siguiente objetivo general: Establecer si la auditoría basada en la norma ISO 27001 mejora los controles de seguridad de la información en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Y además los siguientes objetivos específicos, el primero es establecer si la auditoría basada en la norma ISO 27001, mejora la generación de políticas de seguridad y su cumplimiento en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Y el segundo es establecer si la auditoría basada en la norma ISO 27001, mejora la seguridad física de la infraestructura de TI en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Y el tercero es establecer si la auditoría basada en la norma ISO 27001, mejora la cultura de ciberseguridad en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Estos objetivos nos posibilitan plantear la siguiente hipótesis general: La auditoría basada en la norma ISO 27001 mejora los controles de seguridad de la información en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Y las siguientes hipótesis específicas, la primera es: La auditoría basada en la norma ISO 27001 mejora la

generación de políticas de seguridad y su cumplimiento en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Y la segunda es: La auditoría basada en la norma ISO 27001 mejora la seguridad física de la infraestructura de TI en la Gerencia de informática y tecnología en la municipalidad de Chorrillos. Y la tercera es: La auditoría basada en la norma ISO 27001 mejora la cultura de ciberseguridad en la Gerencia de informática y tecnología en la municipalidad de Chorrillos.

II. MARCO TEÓRICO

Con el objeto de sustentar el presente trabajo se han revisado diferentes precedentes, así como internacionales y nacionales, como precisamos a continuación: A nivel internacional tenemos los siguientes estudios los cuales son:

Maureira (2017), en su investigación titulada “Norma ISO/IEC 27001 aplicada a una carrera universitaria”, el problema que se observó fue la falta de seguridad en la información y 3 principales causas que fueron la tecnología, los procesos y las personas. El objetivo del trabajo fue utilizar la norma ISO 27001 en la carrera universitaria de Ingeniería en Telecomunicaciones en la Universidad Andrés Bello y tuvo como propósito plantear un diseño de SGSI para salvaguardar el cumplimiento de la auditabilidad, disponibilidad, confidencialidad e integridad de la información. El nivel de cumplimiento antes de aplicar la norma se observó en el dominio A5 un 0%, en el dominio A7 un 17% y en el dominio A11 un 67% de su cumplimiento. Y su nivel de cumplimiento luego de aplicar la norma fue en el dominio A5 un 50%, en el dominio A7 un 68% y en el dominio A11 un 67%. El trabajo concluyó que el SGSI genera beneficios para la institución mediante el estándar internacional ISO/IEC 27001:2013, a través del ciclo de mejora continua tales como reducción de riesgos, continuidad del negocio, ahorro de costos.

Así mismo, Paguay y Zamora (2017), en su tesis “Auditoria de la Seguridad Informática basada en la ISO 27001 Sistema de Gestión de Seguridad de la Información para el GAD Municipal de Milagro”, el problema que tenía la institución es que contaba con soluciones tradicionales en el entorno de firewall y antivirus pero que no eran suficientes para poder evitar ataques malintencionados y amenazas latentes, adicional los usuarios y empleados que tenían acceso a la información no poseían una cultura de seguridad. Se evaluó utilizar COBIT, ITIL e ISO 27001, debido a las necesidades de la institución se adoptó por tomar la norma ISO 27001, se determinó controles y métodos sobre los riesgos detectados, en confidencialidad se aseguró que usuarios no autorizados puedan disponer a la información y en flexibilidad donde se pudo adaptar a las áreas de la institución que las necesitaron. En el dominio A5 se observó un 50%, en el dominio A7 un 11,11% y el dominio A11 un 9,09% de cumplimiento. El trabajo concluyó que luego de la definición de los controles y métodos según la norma ISO 27001 orientada a la seguridad se aseguró el activo de información que utiliza el GAD Municipal.

Para Torres (2020), en su trabajo de investigación que lleva por nombre “Plan De Seguridad Informática Basado En La Norma ISO 27001 Para Proteger La Información Y Activos De La Empresa Privada MEGAPROFER S.A.”, donde identificó la problemática en la administración de seguridad de la información y sus activos de información. La ausencia de políticas apropiadas en los procesos y controles son visibles, por esa razón, el personal no toma el cuidado que debería por respetar la reglamentación establecida en la organización. Donde su objetivo fue establecer una propuesta de plan de seguridad informática basada en la norma ISO 27001 en la empresa. Este trabajo propuso una nueva política de seguridad y está diseñada en el marco del cumplimiento institucional para establecer, implementar, mantener y mejorar el proceso de mejora continua que ofrece el SGSI. Los resultados que se obtuvieron después de la aplicación de la norma ISO 27001 son en el indicador disponibilidad un 77,80%, integridad un 75% y en confidencialidad un 75%. Y concluyó que luego de la segunda encuesta que se realizó se logró observar el efecto que obtuvo el cumplimiento del SGSI fue favorable con respecto a la salvaguarda de la confidencialidad, disponibilidad e integridad.

A nivel nacional tenemos los siguientes estudios los cuales son:

El autor Niño (2018), en su tesis titulada “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”, elaborada en la UNPRG, cuyo problema fue la pérdida de los datos a causa de las deficiencias de la capacidad del servidor en donde se preserva los datos obtenidos de las áreas y la perdida de los datos estadísticos sensibles en vista que los usuarios se equivocan y eliminan su información involuntariamente, su objetivo fue diseñar un SGSI para incrementar la disposición, la confianza y la entereza de los activos de información; y mantenibilidad de todos y cada uno de los recursos del proceso crítico, al mismo entre las cuales tiempo que se diagnosticó la postura en curso del aseguramiento de los datos en la organización ODEI Lambayeque en apoyo de preservar los datos. El resultado luego de la utilización de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información permitió identificar los peligros en las

cuales están vulnerables del recurso de información de la organización, seguidamente la estimación de riesgos cuantitativo determinó que su grado de madurez en seguridad de la información en la organización es ínfimo, también se obtuvo en el dominio A5 menor a 10%, en el dominio A7 un 40% y en el dominio A11 un 30% de cumplimiento. El trabajo aportó con la identificación del grado de amenaza en que se encontraba los recursos de información a través del grado de madurez del aseguramiento adoptado y principalmente estimular a los empleados a continuar las normativas y métodos correspondiente a la seguridad informática y sus recursos.

Por otro parte Porras (2019), en su tesis titulada “Sistema De Gestión De Seguridad De La Información Para La Gestión De Riesgos En Activos De Información”, donde se comprobó la ausencia de procesos y procedimientos de seguridad de la información, es decir, la falta de controles de seguridad de la información en la institución es evidente. Donde la finalidad de su investigación fue el de establecer la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riesgos en activos de información en la empresa. La investigación fue acerca del SGSI de la norma ISO 27001 y le proporcionó diferenciar claramente los beneficios de su implementación, de la eficiencia de adaptarlo a los procesos de negocio. Tuvo como resultado que la implantación del SGSI mejoró la madurez de la gestión de riesgos en activos de información y el nivel promedio aumentó de 3,65 a 5,22; Y concluyó que su nivel de madurez mejoró llegando a un estado definido y administrado existiendo una relación clara entre el SGSI y la gestión de riesgos en los activos de información.

Para Chávez y García (2018), en su tesis nombrada “Proceso de auditoría ISO 27001 para la mejora de los controles de seguridad de la información en la Municipalidad Distrital de San Juan Bautista 2018”, indicó como objetivo establecer en qué nivel el proceso de auditoría apoyada en el estándar ISO 27001 reforzará sus controles de seguridad de la información en esta Municipalidad. El problema que presenta es que el departamento de Informática y Telecomunicaciones tenía unas configuraciones de nivel baja en la seguridad informática, por el cual no posee una orden de dar cumplimiento por parte de todas las áreas y/o establecimientos de la institución. Así mismo dispone de ciertas verificaciones de seguridad

informática, de quienes lo administran sin ajustarse a las directrices. Sus resultados nos indican que la significancia entre las variables de estudio es de P= 0,001, que es mejor a 0,05; Y que posibilita concluir que el vínculo del procedimiento de auditoría y el fortalecimiento de los controles de seguridad de la información en la institución pública es relevante.

Los autores Cueva, Lazo, Rodrigez y Andrade (2022), en su artículo titulada "Implementation of Information Security Audit for the Sales System in a Peruvian Company", tuvo como principal objetivo implementar un plan de auditoría basada en la norma ISO 27001 para identificar los problemas encontrados en el sistema de ventas de la organización Domínguez, el problema que observaron fue la falta de personal especializado puesto que se encontró infiltraciones o fallas de seguridad que exponen la información a intrusos informáticos. El método que se utilizó para la auditoría fue la determinación de riesgos y el análisis de la empresa. Los resultados que obtuvieron en los controles de la norma ISO 27001:2014 en un primer momento de 48% para luego terminar en 73% de cumplimiento. El trabajo concluyó que luego de la implementación del plan de auditoría basada en la norma ISO 27001 y la identificación de los problemas de seguridad de la información en la empresa Domínguez se logró una gran mejora en los aspectos de mitigar y reducir los riesgos, lo que se indica un avance significativo en la empresa.

Para un acertado apoyo del presente trabajo de investigación se ha empleado como referencias sobre nuestra problemática, la primera es la auditoría basada en la norma ISO 27001.

Steve G. Watkins (2008) nos indica que la auditoría interna puede utilizarse para muchos fines, pero uno de los principales objetivos de la implantación de un régimen de auditoría interna es controlar la ejecución de los requerimientos del sistema de administración y las prácticas de trabajo. Las auditorías internas son encargadas por la organización, para la organización, y ofrecen la oportunidad relacionada de revisar el nivel de realización del SGSI examinando lo que realmente ocurre en una muestra de eventos y procesos y comparándolo con lo que describe el sistema de gestión documentado (p. 21).

Según Casal (2022) la finalidad de los controles de seguridad de la información es salvaguardar que todos los activos, sistemas, instalaciones, datos y ficheros asociados con la aplicación de la tecnología informática están resguardados respecto al acceso sin autorización, el daño y la utilización incorrecta que sea operable, seguro y protegido en todo momento. Y los principales tipos de controles de seguridad son: directrices y programas de seguridad de tecnología informática, controles de operaciones de TI, controles de administración de seguridad de los empleados, controles de seguridad de los usuarios finales, otorgamiento de perfiles de acceso y contraseñas u otras herramientas de validación de identificación, controles de seguridad organizativos, establecimiento y supervisión de sistemas de medición sobre la fiabilidad de la tecnología informática. La más crítica, y en la que están basadas todas las demás, es la política de seguridad de la tecnología informática.

Otro término a usar es protección de datos, el autor Briceño (2021) en su libro menciona que según el tipo de soporte físico donde se almacenan nuestros datos, las condiciones físicas adversas pueden ser problemáticas o perjudiciales para su integridad. Tales soportes con frecuencia son susceptibles a la temperatura, la humedad, campo magnético, la electricidad, los impactos y otros, cada tipo de entorno tiene sus propias fortalezas y debilidades (p.71).

Por otro lado, International Business Machines [IBM] (2021) define a las políticas de seguridad como una serie de normas aplicables a las operaciones de las entidades y a los instrumentos informativos pertenecientes a una institución. Entre esas normas figuran las relativas a la seguridad física, personal, administrativa y de las redes.

Por otra parte, Laudon y Laudon (2012) definen infraestructura de tecnología de información (TI) a los recursos tecnológicos compartidos que sirven de plataforma a las ejecuciones de sistemas informáticos específicos de las empresas. La infraestructura informática incorpora recursos en hardware, software y servicios como asesoramiento, enseñanza y desarrollo de capacidades que se distribuyen a través de toda la organización o de todos los ámbitos de actividad de la entidad. (p.165).

Según organismos de referencia en materia de seguridad cibernética como ENISA, la cultura de seguridad informática de una institución hace referencia a las experiencias, costumbre, ideas, comportamientos, regulaciones y valores humanos en el tema de seguridad. La cibernética y sus modos se plasman en el comportamiento de los clientes de las tecnologías informáticas.

Para Calderón (2015), la confidencialidad en la seguridad de la información donde refiere que es la necesidad de cuidar o mantener en secreto datos sensibles o recursos para evitar la difusión sin autorización del activo de información. Además, menciona que con respecto a la seguridad de la información la integridad referida a la fidelidad de los datos o de los recursos, generalmente expresada para evitar cambios inapropiados o no autorizados. Finalmente, en el entorno de la seguridad de la información, la disponibilidad significa que la información del sistema debe mantener el acceso a los elementos autorizados, cuyo propósito es evitar la interrupción no autorizada o controlada de los recursos informáticos (p.3).

La metodología de auditoría utilizada como referencia en este trabajo de investigación fue definida por los autores Amogh Phirke y Jayshree Ghorpade-Aher (2019) cuyo objetivo de la auditoría fue comprender las prácticas de revisión del SGSI. El alcance de la auditoría incluyó una evaluación de los servicios, formas y controles de seguridad de la norma ISO 27001 descritos en la documentación del sistema de gestión de seguridad de la información para asegurar la privacidad, fiabilidad y accesibilidad a los activos de la información críticos de la institución dentro del alcance de la misma. Esta auditoría se realizó en cinco fases que se describen a continuación:

Primera fase: Análisis de documentos:

- Identificar el documento básico requerido del SGSI para el proceso y los controles.
- Determinar el tipo, número, ubicación y formato del documento.
- Revisar y registrar la cobertura y las lagunas de la cartera proporcionada.

Segunda fase: Lista de control de la auditoría:

- Identificar los requerimientos obligatorios del SGSI
- Identificar la lista de requisitos documentados de las políticas
- Determinar las áreas prioritarias y las posibles excepciones / anomalías.

Tercera fase: Auditoría del plan:

- Revisar la declaración de alcance para determinar los límites.
- Determinar los elementos primarios y secundarios que se incluirán en la auditoría.
- Determinar el calendario, partes interesadas, los horarios, los tiempos de acceso, entre otros.

Cuarta fase: Realizar una Auditoría:

- Inspecciona muestras o todo el conjunto de activos cuando existe una posible brecha.
- Revisa y observa las características del proceso para las áreas de proceso clave del SGSI.
- Muestra los controles físicos y lógicos para las áreas de riesgo críticas dentro del ámbito del SGSI.

Quinta fase: Informes:

- Resumir las áreas de conformidad, nada de características significativas.
- Crear un hallazgo para cada brecha significativa, anomalía y excepción.
- Desarrollar el informe, asegurando la cobertura de todos los hallazgos en el ámbito de aplicación.

Los estados de los controles del SGSI que se utilizó como referencia en este trabajo de investigación fue definida en el libro de trabajo ISO/IEC 27001:2013 Estado del SGSI, declaración de Aplicabilidad (SoA) y estado de los Controles (2014), el objetivo del libro de trabajo es medir y seguir los elementos requeridos de la norma ISO/IEC 27001. Los estados utilizados se describen a continuación: “Inexistente” Se aplica a los casos en que el sistema de información no está sujeto

a control de seguridad, para “Inicial” Sí, existen salvaguardas, pero no se gestionan y no tienen un procedimiento formal para hacerlas cumplir. Su éxito depende de la suerte y de empleados altamente calificados, el estado “Repetible” donde las medidas de seguridad se implementan de manera completamente informal y la responsabilidad es personal, el estado “definido” es donde el control se realiza de acuerdo con procedimientos escritos, el estado “administrado” es un lugar donde se realiza el control de acuerdo con procedimientos documentados, aprobados y formalizados, por último el estado “optimizado” es donde las pruebas se llevan a cabo de acuerdo con procedimientos documentados, aprobados y formalizados, y su eficacia se mide periódicamente.

Los indicadores que se utilizaron como apoyo en la presente investigación fueron las políticas de seguridad (dominio A5), seguridad física y ambiental (dominio A11) y seguridad ligada a los recursos humanos (dominio A7) basados en la Norma ISO 27001. Con sus respectivas dimensiones normatividad, infraestructura de TI y cultura de ciberseguridad. (Anexo 5)

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1 Tipo de investigación

El proyecto de investigación fue de tipo aplicada ya que el propósito fue la mejora de los controles de seguridad de la información en la gerencia de informática y tecnología, enfocándose en la generación de políticas de seguridad y su cumplimiento, la seguridad física de la infraestructura de TI y la cultura de ciberseguridad. Después de identificar los problemas del gobierno municipal, se realizó la auditoría de acuerdo con la norma internacional ISO 27001 y se brindaron soluciones.

Según Schubert (2017), la investigación aplicada nace desde la práctica de la sociedad y produce resultados que se pueden adoptar, no obstante, estos no forzosamente finalizan en producción, usualmente dado a su importancia. Los resultados son muy significativos para acercar las realizaciones prácticas (p.5).

3.1.2 Diseño de investigación

El diseño de investigación fue experimental de su sub división pre experimental debido a que la investigación se realizó manejando intencionalmente a la variable dependiente (controles de seguridad de información) y se analizaron los eventos en su ámbito natural; Específicamente, nuestras muestras de estudio se analizaron antes de la estimulación y las mismas muestras de estudio se analizaron después.

Hernández, Fernández y Baptista (2014), el diseño preexperimental de una agrupación cuya medida de control es inferior. Frecuentemente es beneficioso como una primera aproximación a la problemática de investigación en la práctica. A una agrupación se le ejecuta una evolución precedente a la estimulación o procesamiento experimental, más adelante se le aplicará el procedimiento seguido de una prueba de post estimulación al final. (p.141).

3.2 Variables y operacionalización

Las variables que dispuso la investigación fueron: Auditoría basada en la norma ISO 27001 como la variable independiente y controles de seguridad de la información como la variable dependiente.

Asimismo, la variable controles de seguridad de la información contiene 3 dimensiones: Normalidad, infraestructura de TI y cultura de ciberseguridad la cual posee tres indicadores que fueron inicial, repetible, definido, administrado y optimizado.

Definición conceptual: Silva, Segadas y Kowask (2014); Los controles de seguridad de la información son una forma de gestionar el riesgo y puede incluir políticas, procedimientos, lineamientos y prácticas de carácter administrativo, técnico, legal o gerencial. Según los requisitos legales y/o las prácticas idóneas de seguridad de la información, ciertos controles pueden considerarse "primeros pasos" en la seguridad de la información en una institución.

Definición operacional: Los controles de seguridad de la información en la Gerencia de informática y tecnología en la municipalidad de Chorrillos mediante una auditoría basada en la norma ISO 27001.

Indicadores: Los indicadores del trabajo fueron inicial, repetible, definido, administrado y optimizado

Escala de medición: Para el trabajo se utilizó el ordinal.

3.3 Población, muestra, muestreo, unidad de análisis

3.3.1 Población

La población la conformaron los 18 servidores públicos de la Gerencia de informática y tecnología de la municipalidad de Chorrillos que laboran durante el 2022.

Criterios de inclusión: Servidores públicos de la gerencia de informática y tecnología de la municipalidad de Chorrillos que laboran durante el año 2022.

Criterios de exclusión: Servidores públicos que no laboren en la Gerencia de informática y tecnología de la municipalidad de Chorrillos que laboran durante el año 2022.

3.3.2 Muestra

La muestra la conformaron los 18 servidores públicos de la gerencia de informática y tecnología de la municipalidad de Chorrillos durante el 2022.

Hernández-Sampieri y Mendoza (2018), “Una muestra es el subgrupo que se considera parte representativa de la población o universo del cual se obtendrán los datos recolectados y la población delineada a partir de la situación de la pregunta investigada.” (p. 196).

3.3.3 Muestreo

El muestreo utilizado fue el no probabilístico.

Arias (2020), “este modelo de muestreo es empleado cuando se desea seleccionar una población teniendo en cuenta sus características comunes o el juicio sesgado del investigador, además, no se utilizan métodos estadísticos de muestreo en este caso y no todos los miembros del grupo poblacional tienen igual posibilidad de ser seleccionado y también se utiliza cuando la población es muy pequeña” (p. 60).

3.4 Técnicas e instrumentos de recolección de datos

La técnica que se empleó en la recopilación de los datos fue la encuesta.

Arias (2022), “Una encuesta es una herramienta realizada mediante un instrumento llamado cuestionario que está orientada únicamente a las personas y aporta información sobre sus puntos de vista, comportamiento o percepciones. De esta forma se pueden obtener resultados cuantitativos o cualitativos, que se enfocan en un problema predeterminado con una secuencia lógica y un sistema de respuesta en escalonada” (p. 112).

Y el instrumento fue el cuestionario.

Para Arias (2020), “Los cuestionarios son herramientas de recolección de información de utilización común en la investigación. Consiste en un conjunto de preguntas formuladas y tabuladas y una gama de posibles respuestas para que respondan los encuestados. No

hay una respuesta correcta o incorrecta, todas las respuestas producen resultados diferentes y se aplican a las multitudes.” (p.21).

Por otro lado, también la técnica que se empleó en la recopilación de los datos fue la observación.

De acuerdo con Flores (2009), “La observación es el procedimiento que usamos con mayor frecuencia en nuestra vida diaria. Estamos constantemente haciendo uso del sentido de la vista para mirar ordinariamente los eventos que se generan en el tiempo de vida. La observación es la manera natural de adquirir conocimiento. Sin embargo, sólo rara vez usamos la observación metódicamente.” (p. 109).

Y el instrumento fue la guía de observación.

En palabras de Campos y Lule (2012). “La guía de observación es una herramienta que posibilita al observador ubicarse sistemáticamente en lo que es en realidad la finalidad del estudio de la investigación, es del mismo modo el soporte que impulsa la recopilación de datos e información de un acontecimiento o fenómeno.” (p.56).

3.5 Procedimientos

En este análisis se determinó uno de los temas recurrentes en la Gerencia de informática y tecnología de la municipalidad Peruana es los controles de seguridad de la información en la entidad pública, por lo que se consideró como variable dependiente para este proyecto, una vez identificado en nuestro enfoque, continuamos investigando situaciones similares en el país y otras instituciones alrededor de todo el mundo para examinar las soluciones que brindaron en ese momento, por otra parte, toda los datos imperantes en la que se basa el proceso como normativas, reglamentos del Estado Peruano; En base a toda la información que el equipo de la gerencia encargada, incluyéndome a mí, se decidió idear una auditoría basada en la norma ISO 27001 para mejorar los controles de seguridad del a información, que es la variable independiente del proyecto de investigación.

Para este análisis se aconseja una investigación exhaustiva de estas 2 variables, para ello se recopilaron diversos trabajos, libros e informes de investigaciones de múltiples especialistas en estos temas

con el fin de comprender el contexto de encontrarse con problemas similares y se consideraron los resultados de sus propuestas de solución, y también gracias a estas investigaciones, obtuvimos un correcto fundamento teórico para respaldar esta investigación, de la cual se derivarán dimensiones y métricas sostenibles. Con la totalidad de los datos se propuso un estudio de aplicación pre experimental, como se implementó este proyecto y se pudo comparar el antes y el después de los indicadores, por otro lado, se conoció a cabalidad las variables y el escenario donde se elaboraron, nos permitió identificar el rango de colaboradores participando en el proyecto, se dispuso de este modo una población y muestreo de representación, adicionalmente se identificó los tipos de muestra que se utilizaron y las técnicas con el objeto de compilar información de indicadores numéricos, se utilizó el juicio de expertos para determinar su validez y se explicó cómo se mide la credibilidad con la ayuda del coeficiente de correlación de Pearson.

De la misma manera determinamos las modalidades de diagnóstico de la información del estudio, los cuales fueron el análisis descriptivo usando la frecuencia del programa SPSS 27 y el estudio deductivo usando el test de normalidad del enfoque de Shapiro-Wilke, que nos dio si el mecanismo tiene difusión de normalidad o no normalidad para su uso de algunas pruebas invariables como el test no paramétrico de Wilcoxon o la prueba paramétrica T-Student a causa de la prueba.

Para la recolección de datos, fue mediante el responsable que trabaja en la gerencia de informática y tecnología, donde brindo información de los controles de seguridad, donde fue recolectado en instrumentos de guía de observación y cuestionario. Brindaron el documento necesario para justificar el permiso de desarrollo del proyecto, esto se aprecia en el ANEXOS.

3.6 Método de análisis de datos

Con el propósito de la evaluación del este trabajo de investigación empleamos el software de estadística SPSS 27, de acuerdo a Green y Salkind (2016) es un software desarrollado por la IBM que lo desarrolló

para la estadística en diferentes instituciones de investigación a nivel mundial, sus rubros abarcan desde la comercialización hasta las ciencias naturales y sus características especiales son su simpleza y perspicaz interfaz y su importe potencial en base de datos (p.162).

Esta investigación aplicó una evaluación descriptiva e inferencial de las variables, en donde la auditoría basada en ISO 27001 (V. Independiente) determinó la influencia de la normatividad, infraestructura de TI y cultura de ciberseguridad en los controles de seguridad de información (V. Dependiente); para este fin se aplicó un pre – test capaz de mostrar la situación preexistente de los indicadores y se procedió a la ejecución de un post - test con los nuevos datos que recibieron los indicadores mediante la aplicación del estándar.

Un análisis de inferencia también se desempeñó sobre la base de la prueba normal a los estados inicial, repetible, definido, administrado y optimizado, ello se realizó con el método Shapiro – Wilk, y determinado por Goss-Sampson (2018) como una forma estadística empleada por JASP para comprobar la suposición de normalidad. Se aplica en las pruebas t para dos muestras independientes y emparejadas. El test aporta un valor de “W”, donde los resultados bajos precisan que el muestreo no está distribuido normalmente, y si sus resultados están menos de un cierto límite puede ser resultados están por debajo de un cierto límite puede ser desestimada (p. 20), dicho método especificó el tipo de distribución de los indicadores del proyecto.

De acuerdo con Shapiro – Wilk se estableció si la asignación es normal o no normal, en el caso de ser ordinario se utilizará la prueba paramétrica T –Student conceptualizada por Lane (2017) como un test de definición de datos estadísticos para el muestreo menor de treinta de asignación ordinario, por el cual se contrasta el promedio y las desviaciones estándar, y se contemplará acertada la hipótesis nula si es mayor a -1,729, es decir el campo de aprobación (p.252) y en la situación de ser no normal, se empleará el test no paramétrica Wilcoxon, es decir estipulado como una prueba no paramétrica que lleva a cabo una

confrontación de promedios entre dos muestras y comprueba su brecha (p.256).

3.7 Aspectos éticos

Este trabajo de investigación está comprometido con lo que dicta la ética basada en las normas que actualmente rigen estos lineamientos alrededor del mundo, busca respetar la propiedad intelectual que pueda ser citada con la debida referencia a los diversos autores como nos indica el manual ISO y la Resolución de junta de la Universidad N°0101-2022/UCV.

Todo esto garantizará la calidad de la investigación y su autenticidad, así como la totalidad de sus datos sean legítimos y verdaderos con el fin de que los eventuales investigadores lean la investigación y contribuyan a futuras investigaciones.

IV.RESULTADOS

En este capítulo se detalla los resultados que se lograron dentro de la investigación haciendo mención a los indicadores de los estados de los dominios A5, A11 y A7. Asimismo, se realizó el procesamiento de los datos, del cual se analizó los resultados de los instrumentos antes y después de realizar la auditoria basada en la norma ISO 27001. El procesamiento de la información se realizó utilizando el SPSS 27, para así determinar si la hipótesis ya planteada se acepta o no:

IV.1 Resultados descriptivos de la investigación

4.1.1 Resultados descriptivos de la normatividad

4.1.1.1 Resultados descriptivos de las políticas de seguridad (dominio A5)

Se llevó a cabo la aplicación del instrumento de investigación (Anexo 10) en un tiempo antes y un tiempo después a la auditoría basada en la norma ISO 27001 en la gerencia de informática y tecnología de la municipalidad de Chorrillos, para validar las políticas de seguridad en la gerencia.

Tabla N°1: *Estado de las políticas de seguridad de la información (dominio A5) para la mejora de generación de políticas de seguridad y su cumplimiento.*

	Estado del dominio A5 - Antes	**Estado del dominio A5 - Después**
Inicial	100,0%	0,0%
Repetible	0,0%	5,6%
Definido	0,0%	94,4%
Administrado	0,0%	0,0%
Optimizado	0,0%	0,0%
Total	100,0%	100,0%

Fuente: Elaboración propia

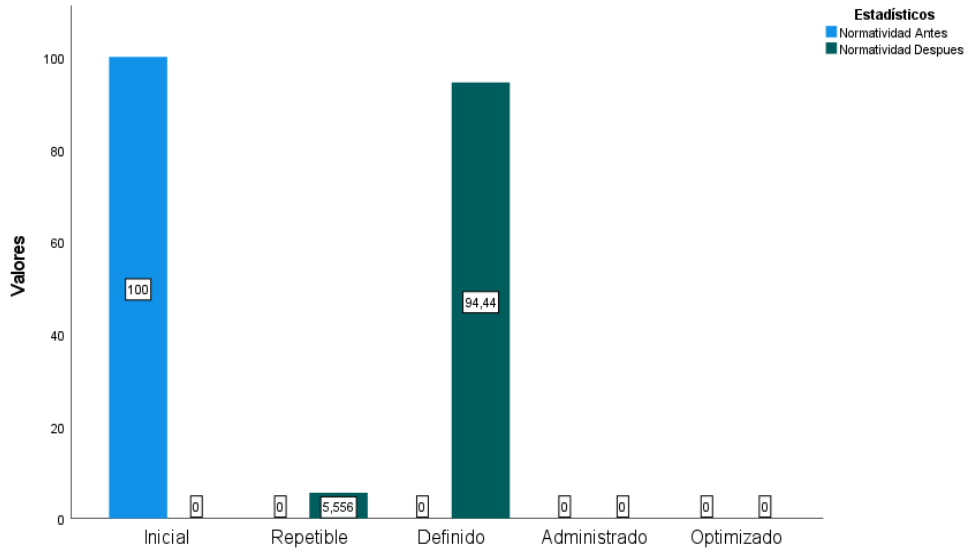


Figura N°1: Estado de las políticas de la seguridad de la información (dominio A5) para la mejora de generación de políticas de seguridad y su cumplimiento.

Fuente: Elaboración propia

Se puede visualizar que el 100% de los controles A5 de la seguridad de la información el estado fue “Inicial” en la gerencia previa al estímulo y este estado nos dio a entender que las políticas existían, pero no se gestionaban, no había un proceso formal para realizarlas y su éxito dependía de tener un personal de alta calidad. Luego de realizar la auditoría, se entregó infografía de los controles de la seguridad de la información y se documentó los controles de seguridad de la información que la norma ISO 27001 nos indica para el aseguramiento de la información. Después del estímulo se pudo visualizar que un 5.56% de los controles del dominio A5 de la seguridad de la información el estado fue “Repetible” este estado nos dio a entender que las medidas de seguridad se realizaban de un modo informal además que la responsabilidad es individual y un 94.44% el estado fue “Definido” por lo que nos indicó que los controles se aplicaron conforme a un procedimiento previamente documentado.

4.1.2. Resultados descriptivos de la seguridad física de la infraestructura de TI

4.1.2.1 Resultados descriptivos de la seguridad física y ambiental (dominio A11)

Se llevó a cabo la aplicación del instrumento de investigación (Anexo 07) en un tiempo antes y un tiempo después a la auditoría basada en la norma ISO 27001 en la gerencia de informática y tecnología de la municipalidad de Chorrillos, para validar la seguridad física y ambiental en la gerencia.

Tabla N°2: *Estado de la seguridad física y ambiental (dominio A11) para la mejora de la seguridad física de la infraestructura de TI.*

	Estado del dominio A11- Antes	**Estado del dominio A11- Después**
Inicial	66,7%	0,0%
Repetible	33,3%	66,7%
Definido	0,0%	33,3%
Administrado	0,0%	0,0%
Optimizado	0,0%	0,0%
Total	100,0%	100,0%

Fuente: Elaboración propia

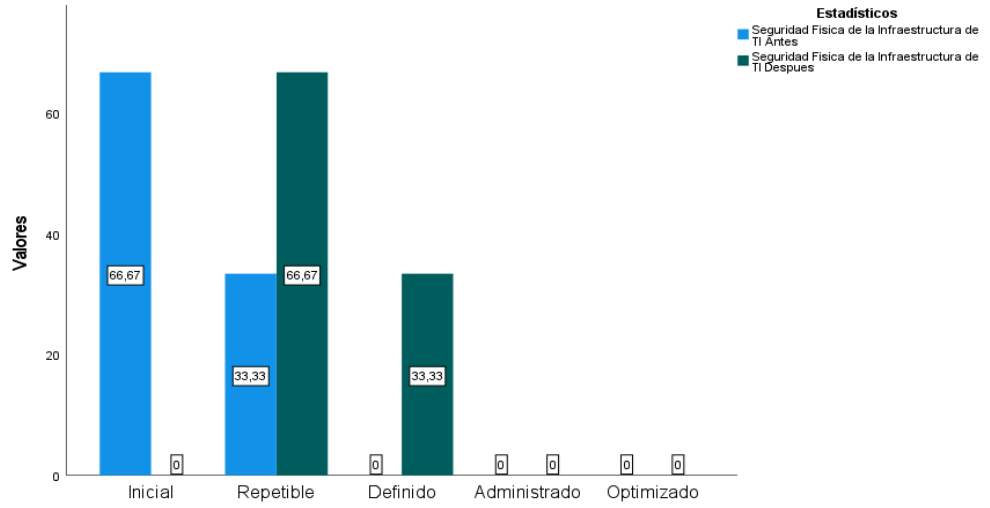


Figura N°2: Estado de la seguridad física y ambiental (dominio A11) para la mejora de la seguridad física de la infraestructura de TI.

Fuente: Elaboración propia

De los servidores públicos de la gerencia encuestados previo al estímulo se pudo visualizar que el 66,67% percibieron que el estado de los controles del dominio A11 de la seguridad de la información fue “Inicial” que nos indicó que las políticas existían, pero no se gestionaban, no había un proceso formal para realizarlas y su éxito dependía de tener un personal de alta calidad y que un 33,33% su estado fue “Repetible” además nos dio a entender que las medidas de seguridad se realizaban de un modo informal además que la responsabilidad es individual. Luego se realizó la auditoría, se entregó infografía de los controles de la seguridad de la información y se documentó los controles de seguridad de la información que la norma ISO 27001 nos indica para el aseguramiento de la información. Después del estímulo se pudo visualizar que un 66,67% de los controles A5 de la seguridad de la información el estado fue “Repetible” a su vez nos dio a entender que las medidas de seguridad se realizaban de un modo informal además que la responsabilidad es individual y un 33,33% el estado fue “Definido” por lo que nos indicó que los controles se aplicaron conforme a un procedimiento previamente documentado.

4.1.3 Resultados descriptivos de la cultura de la ciberseguridad

4.1.3.1 Resultados descriptivos de la seguridad ligada a los recursos humanos (dominio A7)

Se llevó a cabo la aplicación del instrumento de investigación (anexo 07) en un tiempo antes y un tiempo después a la auditoría basada en la norma ISO 27001 en la gerencia de informática y tecnología de la municipalidad de Chorrillos, para validar la seguridad ligada a los recursos humanos.

Tabla N°3: *Estado de la seguridad ligada a los recursos humanos (dominio A7) para la mejora de la cultura de ciberseguridad.*

	Estado del control A11-Antes	Estado del control A11-Después
Inicial	55,6%	0,0%
Repetible	44,4%	55,6%
Definido	0,0%	44,4%
Administrado	0,0%	0,0%
Optimizado	0,0%	0,0%
Total	100,0%	100,0%

Fuente: Elaboración propia

.

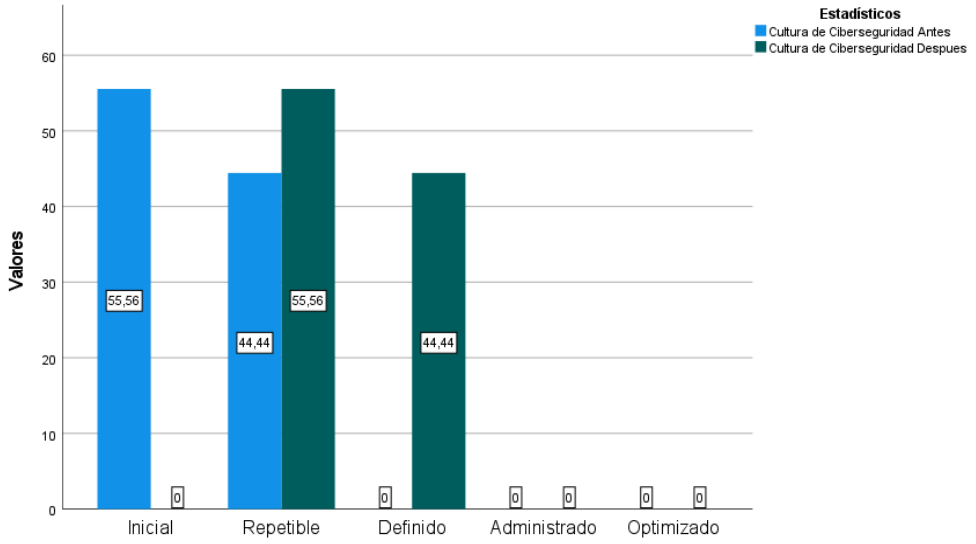


Figura N°3: Estado de la seguridad ligada a los recursos humanos (dominio A7) para la mejora de la cultura de ciberseguridad.

Fuente: Elaboración propia

De los servidores públicos de la gerencia encuestados previo al estímulo se puede visualizar que el 55,56% percibieron que el estado de los controles del dominio A11 de la seguridad de la información fue “Inicial” que nos indicó que las políticas existían, pero no se gestionaban, no había un proceso formal para realizarlas y su éxito dependía de tener un personal de alta calidad y que un 44,44% su estado fue “Repetible” además nos dio a entender que las medidas de seguridad se realizaban de un modo informal además que la responsabilidad es individual. Luego se realizó la auditoría, se entregó infografía de los controles de la seguridad de la información y se documentó los controles de seguridad de la información que la norma ISO 27001 nos indica para el aseguramiento de la información. Después del estímulo se pudo visualizar que un 55,56% de los controles del dominio A11 de la seguridad de la información el estado fue “Repetible” a su vez nos dio a entender que las medidas de seguridad se realizaban de un modo informal además que la responsabilidad es individual y un 44,44% el estado fue “Definido” por

lo que nos indicó que los controles se aplicaron conforme a un procedimiento previamente documentado.

4.1.4 Prueba de Hipótesis

Continuando se muestran las pruebas de hipótesis para cada una de las 3 hipótesis de la presente investigación realizada.

4.1.4.1 Hipótesis específica HE1

HE1-0: La auditoría basada en la norma ISO 27001 no mejora la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de una municipalidad peruana.

HE1-i: La auditoría basada en la norma ISO 27001 mejora la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de una municipalidad peruana.

Se puede visualizar en la tabla 1, el estado del dominio A5 de la seguridad de la información el 100% fue “Inicial” antes de realizar la auditoría basada en la norma ISO 27001. Luego de realizar el estímulo se observa que el estado del dominio A5 de la seguridad de la información un 5,56% fue “Repetible” y un 94,44% fue “Definido”. Por lo tanto, el estado del dominio A5 después del estímulo fue mayor a la del estado antes del estímulo, con lo que se acepta la hipótesis alterna.

4.1.4.2 Hipótesis específica HE2

HE2-0: La auditoría basada en la norma ISO 27001 no mejora la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de una municipalidad peruana.

HE2-i: La auditoría basada en ISO 27001 mejora la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de una municipalidad peruana.

Se puede visualizar en la tabla 2, el estado del dominio A11 de la seguridad de la información el 66,67% fue “Inicial” y 33,33% fue

“Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Luego de realizar el estímulo se observa que el estado del dominio A11 de la seguridad de la información un 66,67% fue “Repetible” y un 33,33% fue “Definido”. Por lo tanto, el estado del dominio A11 después del estímulo fue mayor a la del estado antes del estímulo, con lo que se acepta la hipótesis alterna.

4.1.4.3 Hipótesis específica HE3

HE3-0: La auditoría basada en la norma ISO 27001 no mejora la cultura de ciberseguridad en la gerencia de informática y tecnología de una municipalidad peruana.

HE3-i: La auditoría basada en la norma ISO 27001 mejora la cultura de ciberseguridad en la gerencia de informática y tecnología de una municipalidad peruana.

Se puede visualizar en la tabla 3, el estado del dominio A7 de la seguridad de la información el 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Luego de realizar el estímulo se observa que el estado del dominio A7 de la seguridad de la información un 55,56% fue “Repetible” y un 44,44% fue “Definido”. Por lo tanto, el estado del dominio A7 después del estímulo fue mayor a la del estado antes del estímulo, con lo que se acepta la hipótesis alterna.

4.1.4.4 Hipótesis general

HG-0: La auditoría basada en la norma ISO 27001 no mejora los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana.

HG-i: La auditoría basada en la norma ISO 27001 mejora los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana.

Luego de la revisión de las hipótesis específicas HE1, HE2 y HE3 se puede visualizar que se aceptó todas las hipótesis alternas

HE1-i, HE2-i y HE3-i, por lo tanto, se aceptó la hipótesis general (HG-i).

IV.2 Resultados inferenciales de la investigación

4.2.1 Resultados de prueba de hipótesis de la normatividad

4.2.1.1 Resultados de prueba de hipótesis de las políticas de la seguridad (dominio A5)

Para el presente estudio se utilizó la prueba de Shapiro-Wilk para el análisis del comportamiento de distribución de los datos de interés, debido a que la información es menor a 50 para la dimensión de normalidad.

Tabla N°4: *Prueba de normalidad del dominio A5*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Normatividad Antes	.	18	.	.	18	.
Normatividad Después	,538	18	,000	,253	18	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia

Tabla N°4 donde se pudo observar, la significación asintótica bilateral (sig) que fue igual a 0,000; por lo tanto, es menor a 0,05 entonces, se tuvo que aplicar la prueba WILCOXON para muestras relacionadas.

Tabla N°5: *Prueba de Wilcoxon del dominio A5*

Estadísticos de prueba[a]	
	Normatividad Después - Normatividad Antes
Z	-4,146[b]
Sig. asin. (bilateral)	,000

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

Fuente: Elaboración propia

En la tabla N°5 donde se pudo observar que el valor crítico de la prueba fue de sig = 0,000 < 0,05, se rechaza la hipótesis nula y se acepta la alternativa, dando como resultado que: La auditoría basada en la norma ISO 27001 mejora la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de una municipalidad peruana.

4.2.2 Resultados de prueba de hipótesis de la seguridad física de la infraestructura de TI

4.2.2.1 Resultados de prueba de hipótesis de la seguridad física y ambiental (dominio A11)

Para el presente estudio se utilizó la prueba de Shapiro-Wilk para el análisis del comportamiento de distribución de los datos de interés, debido a que la información es menor a 50 para la dimensión de normalidad.

Tabla N°6: *Prueba de normalidad del dominio A11*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Seguridad Física de la Infraestructura de TI Antes	,421	18	,000	,601	18	,000
Seguridad Física de la Infraestructura de TI Despues	,421	18	,000	,601	18	,000

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia

Tabla N°6 donde se pudo observar, la significación asintótica bilateral (sig) fue igual a 0,000; por lo tanto, es menor a 0,05 entonces, se tuvo que aplicar la prueba WILCOXON para muestras no relacionadas.

Tabla N°7: *Prueba de Wilcoxon del dominio A11*

Estadísticos de prueba[a]	
	Seguridad Física de la Infraestructura de TI Después - Seguridad Física de la Infraestructura de TI Antes
Z	-4,243[b]
Sig. asin. (bilateral)	,000
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Fuente: Elaboración propia

En la tabla N°7 donde se pudo observar que el valor crítico de la prueba fue de sig = 0,000 < 0,05, se rechaza la hipótesis nula y se acepta la alternativa, dando como resultado que: La auditoría basada en ISO 27001 mejora la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de una municipalidad peruana.

4.2.3 Resultados de prueba de hipótesis de la cultura de la ciberseguridad

4.2.3.1 Resultados de prueba de hipótesis del estado del dominio A7 de seguridad de la información

Para el presente estudio se utilizó la prueba de Shapiro-Wilk para el análisis del comportamiento de distribución de los datos de interés, debido a que la información es menor a 50 para la dimensión de normalidad.

Tabla N°8: *Prueba de normalidad del dominio A7*

Pruebas de normalidad						
	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Cultura de Ciberseguridad Antes	,363	18	,000	,638	18	,000
Cultura de Ciberseguridad Después	,363	18	,000	,638	18	,000
a. Corrección de significación de Lilliefors						

Fuente: Elaboración propia

Tabla N°8 donde se ha podido observar, la significación asintótica bilateral (sig) es igual a 0,000; por lo tanto, es menor a 0,05 entonces, se tendrá que aplicar la prueba WILCOXON para muestras no relacionadas.

Tabla N°9: *Prueba de Wilcoxon del dominio A7*

Estadísticos de prueba[a]	
	Cultura de Ciberseguridad Después - Cultura de Ciberseguridad Antes
Z	-4,243[b]
Sig. asin. (bilateral)	<.001
a. Prueba de rangos con signo de Wilcoxon	
b. Se basa en rangos negativos.	

Fuente: Elaboración propia

En la tabla N°9 se puede ver que el valor crítico de la prueba fue de sig < 0,001 < 0,05, se rechaza la hipótesis nula y se acepta la alternativa,

dando como resultado que: La auditoría basada en la norma ISO 27001 mejora la cultura de ciberseguridad en la gerencia de informática y tecnología de una municipalidad peruana.

4.2.4 Hipótesis general inferencial

HG-0: La auditoría basada en la norma ISO 27001 no mejora los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana.

HG-i: La auditoría basada en la norma ISO 27001 mejora los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana.

Luego de la revisión de las hipótesis específicas HE1, HE2 y HE3 se puede visualizar que se aceptaron todas las hipótesis HE1, HE2 y HE3, por lo tanto, se aceptó la hipótesis general alterna (HG-i).

V. DISCUSIÓN

En general, los estados de los 3 dominios de seguridad de la información obtuvieron un efecto relevante para la mejora de los controles de seguridad de la información en la gerencia de informática y tecnología en la municipal de Chorrillos. Ya que se logró en las políticas de seguridad (dominio A5) un 5,56% en el estado “Repetible” y 94,44% en el estado “Definido”. Por su parte en la seguridad física y ambiental (dominio A11) un 66,67% en estado “Repetible” y 33,33% en “Definido”. Y por último en la seguridad ligada a los recursos humanos (dominio A7) un 55,56% en estado “Repetible” y 44,44% en estado “Definido”. Con estos resultados se evidencio que a través de la auditoría basado en la norma ISO 27001 se generan políticas de seguridad, se mejora la seguridad física de la infraestructura de TI y se mejora la cultura de ciberseguridad. A continuación, estos resultados se contrastaron con trabajos similares para cada indicador.

El estado de las políticas de seguridad de la información (dominio A5) tuvo un cambio favorable pasando de un estado “Inicial” de 100% al 5,56% en estado “Repetible” y un 94,44% en estado “Definido”. En este contexto Maureira (2017), aplicó la norma ISO 27001 en la carrera universitaria de Ingeniería en Telecomunicaciones en la Universidad Andrés Bello donde obtuvo como primer resultado sobre el cumplimiento del dominio A5 un 0% para luego de aplicar la norma se observó un 50% del cumplimiento. El resultado de Maureira (2017) fue diferente ya que se evaluó el cumplimiento del dominio A5 basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado del dominio.

El estado de la seguridad física y ambiental (dominio A11) tuvo un cambio relevante, donde en el pretest se obtuvo un 66,67% fue “Inicial” y 33,33% fue “Repetible” para luego un 66,67% fue “Repetible” y un 33,33% fue “Definido”. Igualmente, Maureira (2017), utilizó la norma ISO 27001 en la carrera universitaria de Ingeniería en Telecomunicaciones en la Universidad Andrés Bello donde consiguió como primer resultado sobre el estado del dominio A11 de 67% para luego 67% el su cumplimento después de aplicar la norma. El resultado de Maureira (2017) fue diferente al presente trabajo de investigación ya que se evaluó el estado del dominio A11 basada en la norma ISO 27001.

El estado de la seguridad ligada los recursos humanos (dominio A7) se obtuvo una mejora notable, donde antes de aplicar el estímulo los datos que se obtuvieron fueron los siguientes de un estado de 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Posteriormente el estado del dominio A7 de la seguridad de la información fue un 55,56% en “Repetible” y un 44,44% en “Definido”. De igual modo Maureira (2017), donde su objetivo del trabajo tuvo como finalidad proponer un diseño de SGSI para asegurar el cumplimiento de la auditabilidad, disponibilidad, confidencialidad e integridad de la información. Donde obtuvo como resultado de cumplimiento en el dominio A7 de 17% antes de la estimulación para luego obtener un 68% de cumplimiento del dominio basado en la norma ISO 27001. El resultado de Maureira (2017) fue diferente ya que se evaluó el cumplimiento del dominio A7 basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado del dominio.

El estado de las políticas de seguridad (dominio A5) tuvo un cambio favorable pasando de un estado “Inicial” de 100% al 5,56% en estado “Repetible” y un 94,44% en estado “Definido”. En este contexto Paguay y Zamora (2017), Se evaluó utilizar COBIT, ITIL e ISO 27001, debido a las necesidades de la institución se adoptó por tomar la norma ISO 27001 donde obtuvo como resultado sobre el cumplimiento del dominio A5 un 50%. El resultado de Paguay y Zamora (2017) fue diferente ya que se evaluó el cumplimiento del dominio A5 basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado del dominio.

El estado de la seguridad física y ambiental (dominio A11) tuvo un cambio relevante, donde en el pretest se obtuvo un 66,67% fue “Inicial” y 33,33% fue “Repetible” para luego un 66,67% fue “Repetible” y un 33,33% fue “Definido”. Igualmente, Paguay y Zamora (2017), Se evaluó utilizar COBIT, ITIL e ISO 27001, debido a las necesidades de la institución se adoptó por tomar la norma ISO 27001 donde obtuvo como resultado sobre el cumplimiento del dominio A11 un 9,09%. El resultado fue diferente ya que el presente trabajo de investigación evaluó el estado del dominio A11 a diferencia de Paguay y Zamora (2017) que evaluó el cumplimiento del dominio A11 basada en la norma ISO 27001.

El estado de la seguridad ligada a los recursos humanos (dominio A7) se obtuvo una mejora notable, donde antes de aplicar el estímulo los datos que se obtuvieron fueron los siguientes de un estado de 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Posteriormente el estado del dominio A7 de la seguridad de la información fue un 55,56% en “Repetible” y un 44,44% en “Definido”. De igual modo Paguay y Zamora (2017), Se evaluó utilizar COBIT, ITIL e ISO 27001, debido a las necesidades de la institución se adoptó por tomar la norma ISO 27001 donde obtuvo como resultado sobre el cumplimiento del dominio A7 un 11,11%. El resultado de Paguay y Zamora (2017) fue diferente ya que se evaluó el cumplimiento del dominio A7 basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado del dominio.

El estado de las políticas de seguridad (dominio A5) tuvo un cambio favorable pasando de un estado “Inicial” de 100% al 5,56% en estado “Repetible” y un 94,44% en estado “Definido”, en el estado de la seguridad física y ambiental (dominio A11) tuvo un cambio relevante, donde en el pretest se obtuvo un 66,67% fue “Inicial” y 33,33% fue “Repetible” para luego un 66,67% fue “Repetible” y un 33,33% fue “Definido” y El estado de la seguridad ligada a los recursos humanos (dominio A7) se obtuvo una mejora notable, donde antes de aplicar el estímulo los datos que se obtuvieron fueron los siguientes de un estado de 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Posteriormente el estado del dominio A7 de la seguridad de la información fue un 55,56% en “Repetible” y un 44,44% en “Definido”. En este contexto Torres (2020), donde su objetivo fue elaborar una propuesta de plan de seguridad informática utilizando la norma ISO 27001 en la empresa MEGAPROFER donde obtuvo como resultado con respecto a la disponibilidad un 77,80%, integridad un 75% y en confidencialidad un 75%. El resultado de Torres (2020) fue diferente ya que se evaluó los indicadores de disponibilidad, integridad y confidencialidad basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado de los dominios A5, A11 y A7 de la norma.

El estado de las políticas de seguridad (dominio A5) tuvo un cambio favorable pasando de un estado “Inicial” de 100% al 5,56% en estado “Repetible” y

un 94,44% en estado “Definido”. En este contexto Niño (2018), su objetivo fue diseñar un SGSI para incrementar la disposición, la confianza y la entereza de los activos de información; y mantenibilidad de todos y cada uno de los recursos del proceso crítico, al mismo entre las cuales tiempo que se diagnostica la postura en curso del aseguramiento de los datos en la organización ODEI Lambayeque en apoyo de preservar los datos donde obtuvo como resultado sobre el cumplimiento del dominio A5 menor a 10%. El resultado de Niño (2018) fue diferente ya que se evaluó el cumplimiento del dominio A5 basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado del dominio.

El estado de la seguridad física y ambiental (dominio A11) tuvo un cambio relevante, donde en el pretest se obtuvo un 66,67% fue “Inicial” y 33,33% fue “Repetible” para luego un 66,67% fue “Repetible” y un 33,33% fue “Definido”. Igualmente, Niño (2018), su objetivo fue diseñar un SGSI para incrementar la disposición, la confianza y la entereza de los activos de información; y mantenibilidad de todos y cada uno de los recursos del proceso crítico, al mismo entre las cuales tiempo que se diagnostica la postura en curso del aseguramiento de los datos en la organización ODEI Lambayeque en apoyo de preservar los datos donde obtuvo como resultado sobre el cumplimiento del dominio A11 un 30%. El resultado fue diferente ya que el presente trabajo de investigación evaluó el estado del dominio A11 a Niño (2018) que evaluó el cumplimiento del dominio A11 basada en la norma ISO 27001.

El estado de la seguridad ligada a los recursos humanos (dominio A7) se obtuvo una mejora notable, donde antes de aplicar el estímulo los datos que se obtuvieron fueron los siguientes de un estado de 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Posteriormente el estado del dominio A7 de la seguridad de la información fue un 55,56% en “Repetible” y un 44,44% en “Definido”. De igual modo Niño (2018), su objetivo fue diseñar un SGSI para incrementar la disposición, la confianza y la entereza de los activos de información; y mantenibilidad de todos y cada uno de los recursos del proceso crítico, al mismo entre las cuales tiempo que se diagnostica la postura en curso del aseguramiento de los datos en la organización ODEI Lambayeque en apoyo de preservar los datos donde obtuvo como resultado sobre

el cumplimiento del dominio A7 un 40%. El resultado de Niño (2018) fue diferente ya que se evaluó el cumplimiento del dominio A7 basada en la norma ISO 27001 a diferencia del presente trabajo de investigación que evaluó el estado del dominio.

El estado de las políticas de seguridad (dominio A5) tuvo un cambio favorable pasando de un estado “Inicial” de 100% al 5,56% en estado “Repetible” y un 94,44% en estado “Definido”, en el estado de la seguridad física y ambiental (dominio A11) tuvo un cambio relevante, donde en el pretest se obtuvo un 66,67% fue “Inicial” y 33,33% fue “Repetible” para luego un 66,67% fue “Repetible” y un 33,33% fue “Definido” y El estado de la seguridad ligada a los recursos humanos (dominio A7) se obtuvo una mejora notable, donde antes de aplicar el estímulo los datos que se obtuvieron fueron los siguientes de un estado de 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Posteriormente el estado del dominio A7 de la seguridad de la información fue un 55,56% en “Repetible” y un 44,44% en “Definido”. En este contexto Porras (2019), cuyo objetivo de su investigación fue el de determinar la influencia de la implementación del Sistema de Gestión de Seguridad de la Información en la gestión de riesgos en activos de información en la Empresa de BPO Contac Center Digitex, Lima donde obtuvo como resultado con respecto a la madurez de la gestión de riesgos en activos de información un valor promedio de 3,65 a 5,22. El resultado de Porras (2019) fue diferente ya que se evaluó el nivel de madurez de la gestión de riesgos en activos de información a diferencia del presente trabajo de investigación que evaluó el estado de los dominios A5, A11 y A7 de la norma ISO 27001.

El estado de las políticas de seguridad (dominio A5) tuvo un cambio favorable pasando de un estado “Inicial” de 100% al 5,56% en estado “Repetible” y un 94,44% en estado “Definido”. En este contexto Cueva (2022), quienes realizaron un plan de auditoría y seguridad de la información utilizando la norma ISO 27001 para un sistema de ventas para la mejora de la seguridad informática obteniendo en un inicio 50% del cumplimiento del dominio A5 para el final obteniendo un 65% en la misma. El resultado de Cueva (2022) fue diferente en esta investigación, puesto que aplicaron el plan de auditoría para mejorar el sistema de ventas de la

empresa peruana, utilizando la metodología de cinco etapas de gestión de proyectos evaluando su cumplimiento.

El estado de la seguridad física y ambiental (dominio A11) tuvo un cambio relevante, donde en el pretest se obtuvo un 66,67% fue “Inicial” y 33,33% fue “Repetible” para luego un 66,67% fue “Repetible” y un 33,33% fue “Definido”. Para Igualmente, Cueva (2022), quienes, al realizar las cinco etapas de gestión de proyectos, explicación del procedimiento y definición de cada etapa a través de la norma ISO 27001 obtuvieron como resultado del Dominio A11 en un inicio un 45% de su cumplimiento, para luego de aplicar la auditoría y el uso de la Norma obtuvieron un 77% de su cumplimiento. El resultado de Cueva (2022) a diferencia de esta investigación se pudo aplicar todos los dominios de la Norma ISO 27001 donde se busca el cumplimiento de la misma, por ello se puedo observar una clara mejora después de aplicar la metodología.

El estado de la seguridad ligada a los recursos humanos (dominio A7) se obtuvo una mejora notable, donde antes de aplicar el estímulo los datos que se obtuvieron fueron los siguientes de un estado de 55,56% fue “Inicial” y 44,44% fue “Repetible” antes de realizar la auditoría basada en la norma ISO 27001. Posteriormente el estado del dominio A7 de la seguridad de la información fue un 55,56% en “Repetible” y un 44,44% en “Definido”. De igual modo Cueva (2022), quienes tuvieron como objetivo implementar un plan de auditoría y seguridad de la información utilizando la norma ISO 27001 para un sistema de ventas en una empresa peruana lograron tener resultados notables del dominio A7 pasando de un 50% a un 73% del cumplimiento de los controles de seguridad de la información. Ambas investigaciones evidencian que el recurso humano es fundamental para realizar un aseguramiento de la información y que es importante difundir y hacer de conocimiento a los empleados sobre los controles de seguridad de la información para mejorar el sistema de gestión de seguridad de la información.

VI. CONCLUSIONES

Como resultado de este trabajo se obtuvieron las siguientes conclusiones:

Primera: Se estableció que la auditoría basada en la norma ISO 27001 mejora los controles de seguridad de la información en la gerencia de informática y tecnología de la municipalidad de Chorrillos. Donde se evaluó los factores clave de la normatividad, la seguridad física de la infraestructura de TI y la cultura de ciberseguridad para logrando los resultados deseados en beneficio a la gerencia.

Segunda: Con respecto a la normatividad se estableció que la auditoría basada en la norma ISO 27001 mejora la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de la municipalidad de Chorrillos. Ya que se logró alcanzar una mejora en las políticas de la seguridad (dominio A5) de 5,56% en el estado “Repetible” y 94,44% en el estado “Definido”.

Tercera: Por su parte de la infraestructura de TI se estableció que la auditoria basada en la norma ISO 27001 mejora la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de la municipalidad de Chorrillos. Ya que se logró alcanzar una mejora en la seguridad física y ambiental (dominio A11) un 66,67% en estado “Repetible” y 33,33% en estado “Definido”.

Cuarta: Por último, en la cultura de ciberseguridad se estableció que la auditoria basada en la norma ISO 27001 mejora la cultura de ciberseguridad en la gerencia de informática y tecnología de la municipalidad de Chorrillos. Ya que se logró alcanzar una mejora en la seguridad ligada a los recursos humanos (dominio A7) un 55,56% en estado “Repetible” y 44,44% en estado “Definido”.

VII. RECOMENDACIONES

A continuación, se enumeran una serie de recomendaciones cuya implementación son vitales para mejorar los controles de seguridad en la gerencia de informática y tecnología de la municipalidad de Chorrillos.

Primera: Se recomienda que la gerencia de informática y tecnología de la municipalidad de Chorrillos continúe realizando auditorías a los controles de seguridad de la información basada en la norma ISO 27001 en todas las áreas para poder seguir brindando a los usuarios los servicios que esperan de la institución.

Segunda: Se aconseja que la gerencia de informática y tecnología impulse una reforma sobre la seguridad física de su infraestructura de TI, definiendo la seguridad como prioridad a todo dispositivo que tenga acceso a la información como también a su entorno de los mismos.

Tercera: Se sugiere que la gerencia de informática y tecnología lleve a cabo más capacitaciones continuas sobre temas de control de seguridad de la información y ciberseguridad para así lograr una fuerza laboral bien capacitada y pueda lograr las metas de la municipalidad.

Cuarta: Finalmente se recomienda la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 en toda la institución para mejorar sus procesos y permitirle alcanzar sus objetivos estratégicos municipales aprovechando las condiciones favorables que existen actualmente.

REFERENCIAS

ARIAS, José. *Técnicas e Instrumentos De Investigación Científica*. Arequipa: Enfoques Consulting EIRL, 2020. 171 pp. ISBN: 978-612-48444-0-9

ARIAS, J., HOLGADO, J., TAFUR, T. y VASQUEZ, M., 2022. *Metodología de la investigación: El método ARIAS para desarrollar un proyecto de tesis*. Perú: Instituto universitario de Innovación ciencia y Tecnología Inudi Perú S.A.C. 2022. 162 pp. ISBN 9786125069047. DOI: https://doi.org/10.35622/inudi.b.016

CASTILLO, Roxana. Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013. Tesis (Titulada en Ingeniería de Sistemas). Huaraz: Universidad Católica los Ángeles Chimbote, 2019. Disponible en: http://repositorio.uladech.edu.pe/bitstream/handle/20.500.13032/11993/SGSI_CASTILLO_COLLAZOS_ROXANA_ELIDA.pdf?sequence=4

CAMPOS, G. y Lule, N. E. (2012). La observación, un método para el estudio de la realidad. Xihmai, 7(13), 45-60. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=3979972. ISSN 1870_6703

CHAVEZ COBOS, Linder y GARCIA GUERREO, Rudy, 2018. Proceso de auditoria ISO 27001 para la mejora de los controles de seguridad de la información en la municipalidad distrital de san juan bautista 2018. Tesis (Presentada para optar el título profesional en ciencias e ingeniería con mención en ingeniería de sistemas de información). Loreto: Universidad Científica del Perú. Disponible en: http://repositorio.ucp.edu.pe/handle/UCP/1292

CORDERO, J.V., 2021. ISO/IEC standards as mechanisms of proactive responsibility in the General Data Protection Regulation. *Revista de Internet, Derecho y Política*, vol. 33, no. 33, pp. 1-12. ISSN 16998154. DOI 10.7238/IDP.V0I33.376366.

Cueva Ruiz, L., Lazo Amado, M., Rodrigez Carrasco, J., & Andrade-Arenas, L. (2022). Implementation of Information Security Audit for the Sales System in a Peruvian Company. 12(3). ISSN 20885334.

CULOT, G., NASSIMBENI, G., PODRECCA, M. y SARTOR, M., 2021. The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, vol. 33, no. 7, pp. 76-105. ISSN 17542731. DOI 10.1108/TQM-09-2020-0202.

ESKALUSPITA, A.Y., 2020. ISO 27001:2013 for Laboratory Management Information System at School of Applied Science Telkom University. IOP Conference Series: Materials Science and Engineering, vol. 879, no. 1, pp. 0-6. ISSN 1757899X. DOI 10.1088/1757-899X/879/1/012074.

FAJAR, A.N., CHRISTIAN, H. y GIRSANG, A.S., 2018. Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. *Journal of Physics: Conference Series*, vol. 1090, no. 1, pp. 0-9. ISSN 17426596. DOI 10.1088/1742-6596/1090/1/012060.

FLORES, R. (2009). Observando observadores: Una introducción a las técnicas cualitativas de investigación social. Santiago: Ediciones Universidad Católica de Chile. ISBN N°978-956-14-1094-7

GREEN, Samuel y SALKIND, Neil. Using SPSS for Windows and Macintosh, Books a la Carte [en línea]. Pearson: ACM. 8th Edition. ISBN: 978-0-13-431988-9. 2016. [Fecha de consulta: 20 de mayo de 2020]. Disponible en: https://dl.acm.org/doi/book/10.5555/3066228.

GUNAWAN, N.K., HADIPRAKOSO, R.B. y KABETTA, H., 2020. Comparative study between the integration of ITIL and ISO / IEC 27001 with the integration of COBIT and ISO / IEC 27001. *IOP Conference Series: Materials Science and Engineering*, vol. 852, no. 1. ISSN 1757899X. DOI 10.1088/1757-899X/852/1/012128.

Hernández-Sampieri, R. & Mendoza, C (2018). Metodología de la investigación. Las rutas cuantitativa, cualitativa y mixta, Ciudad de México, México: Editorial Mc Graw Hill Education, Año de edición: 2018, ISBN: 978-1-4562-6096-5.

HOFMANN, M. y HOFMANN, A., 2017. ISMS-Tools zur Unterstützung eines nativen ISMS gemäß ISO 27001. *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft fur Informatik (GI)*, vol. 275, pp. 1617-1629. ISSN 16175468. DOI 10.18420/in2017_162.

IBM docs. IBM - Deutschland | IBM [en línea]. [sin fecha] [consultado el 15 de junio de 2022]. Disponible en: https://www.ibm.com/docs/es/i/7.3?topic=security-policy-objectives.

ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap analysis) workbook. Disponible en: https://www.iso27001security.com/

KURNIANTO, A., ISNANTO, R. y WIDODO, A.P., 2018. Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center in Ministry of Internal Affairs. *E3S Web of Conferences*, vol. 31, pp. 0-5. ISSN 22671242. DOI 10.1051/e3sconf/20183111013.

Laudon K.y Laudon J. (2016) “Sistemas de Información Gerencial” Editorial Pearson. México ISBN: 978-607-32-3696-6. 680 páginas. 14º Edición.

Longras, T. Pereira, P. Carneiro and P. Pinto, "On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations," 2018 International Conference on Intelligent Systems (IS), 2018, pp. 886-890, doi: 10.1109/IS.2018.8710558.

MARIO G. PIATTINI VELTHUIS. Mantenimiento y Evolución de Sistemas de información. Madrid: RA-MA Editorial, 2018. ISBN 9788499647869. Disponible en:

https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2498297&lang=es&site=eds-live

MARTELO, R.J., MADERAY, J.E. y BETÍN, A.D., 2015. Software para gestión documental, un componente modular del Sistema de Gestión de Seguridad de la Información (SGSI). *Información Tecnológica*, vol. 26, no. 2, pp. 129-134. ISSN 07180764. DOI 10.4067/S0718-07642015000200015.

Maureira Sánchez, Daniel, 2017.NORMA ISO/IEC 27001 APLICADA A UNA CARRERA UNIVERSITARIA. Chile: Universidad ANDRES BELLO. Disponible en: https://repositorio.unab.cl/xmlui/bitstream/handle/ria/3720/a118929_Maureira_D_Norma_ISO_IEC_27001_aplicada_2017_Tesis.pdf?sequence=1&isAllowed=y.

MONTEZA MERA, Lisbet, 2019. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO / IEC 27001: 2013 para la Municipalidad Distrital de El Agustino. [en línea], pp. 1-370. Lima: Universidad Peruana De Ciencias Aplicadas. Disponible en: https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/652121/Monteza_ML.pdf?sequence=3.

NIÑO MORANTE, Nilton, 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. Tesis (Presentada para optar el grado académico de maestro en Ingeniería de Sistemas). Lambayeque: Universidad Nacional “Pedro Ruiz Gallo”, Escuela de Postgrado. Disponible en: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y.

NPT-ISO/IEC 27001:2014. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª. Edición.

PAGUAY LEMA, Cinthya y ZAMORA ARANA, Gabriel,2017. Auditoria de la seguridad informática basado en la ISO 27001 sistema de gestión de seguridad de la información para el GAD Municipal de Milagro. Proyecto de grado previo a la obtención del título de ingeniero en sistemas computacionales. Ecuador: Universidad estatal de Milagro facultad ciencias de la ingeniería. Disponible en: https://repositorio.unemi.edu.ec/handle/123456789/3845?locale=es

PANE, S.F. y MAULANA, R., 2019. Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001: 2013., DOI 10.1088/1742-6596/1196/1/012033.

PHIRKE, A. y GHORPADE-AHER, J., 2019. Best Practices of Auditing in an Organization using ISO 27001 Standard., Retrieval Number: B11280782S319/19©BEIESP DOI: 10.35940/ijrte. B1128.0782S319

Porras Ruiz, Miguel, 2019. Sistema De Gestión De Seguridad De La Información Para La Gestión De Riesgos En Activos De Información. Huancayo: Universidad Peruana Los Andes. Disponible en: https://repositorio.upla.edu.pe/handle/20.500.12848/2604.

PRAPENAN, G.G. y PAMUJI, G.C., 2020. Information System Security Analysis of XYZ Company Using COBIT 5 Framework and ISO 27001:2013. *IOP Conference Series: MaterialsScience and Engineering*, vol. 879, no. 1, pp. 0-6. ISSN 1757899X. DOI 10.1088/1757-899X/879/1/012047.

¿Qué son los controles de seguridad de TI? Auditool: Red Global de Conocimientos en Auditoría y Control Interno [en línea]. [consultado el 1 de julio de 2022]. Disponible en: https://www.auditool.org/blog/auditoria-de-ti/8317-que-son-los-controles-de-seguridad-de-ti

ROSA, F.D.F., JINO, M., MARCOS, P., BUENO, S., BONACIN, R., ARCHER, C.T.I.R. y SP, C., 2019. Applying heuristics to the selection and prioritisation of security assessment items in software assessment: the case of ISO / IEC 27001., vol. 8, no. 2, pp. 12-20.

SILVA, C.F.E, SEGADAS, A. L.G. y KOWASK B.A.E., [2014]. Gestión de la seguridad de la información. S.l.: ISBN: (ebook)

SUSSY, B., WILBER, C., MILAGROS, L. y CARLOS, M., 2015. ISO/IEC 27001 implementation in public organizations: A case study. *2015 10th Iberian Conference on Information Systems and Technologies, CISTI 2015*, DOI 10.1109/CISTI.2015.7170355.

TALIB, M.A., KHELIFI, A. y UGURLU, T., 2012. Using ISO 27001 in teaching information security. *IECON Proceedings (Industrial Electronics Conference)*, pp. 3149-3153. DOI 10.1109/IECON.2012.6389395.

TORRES CHANGO, Christian, 2020. Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada MEGAPROFER S.A. Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos. Ecuador: Universidad Técnica De Ambato. Facultad De Ingeniería En Sistemas, Electrónica E Industrial. Disponible en: https://repositorio.uta.edu.ec/handle/123456789/30690

VALENCIA-DUQUE, F.J. y OROZCO-ALZATE, M., 2017. Las normas de reciente publicación de ISO incorporan dos elementos comunes. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, no. 22, pp. 73-88. ISSN 16469895. DOI 10.17013/risti.22.73.

VEGA BRICEÑO, Edgar. Seguridad de la información [en línea]. Editorial Científica 3Ciencias, 2021. ISBN 9788412209365 [consultado el 15 de junio de 2022]. Disponible en: doi:10.17993/tics.2021.4

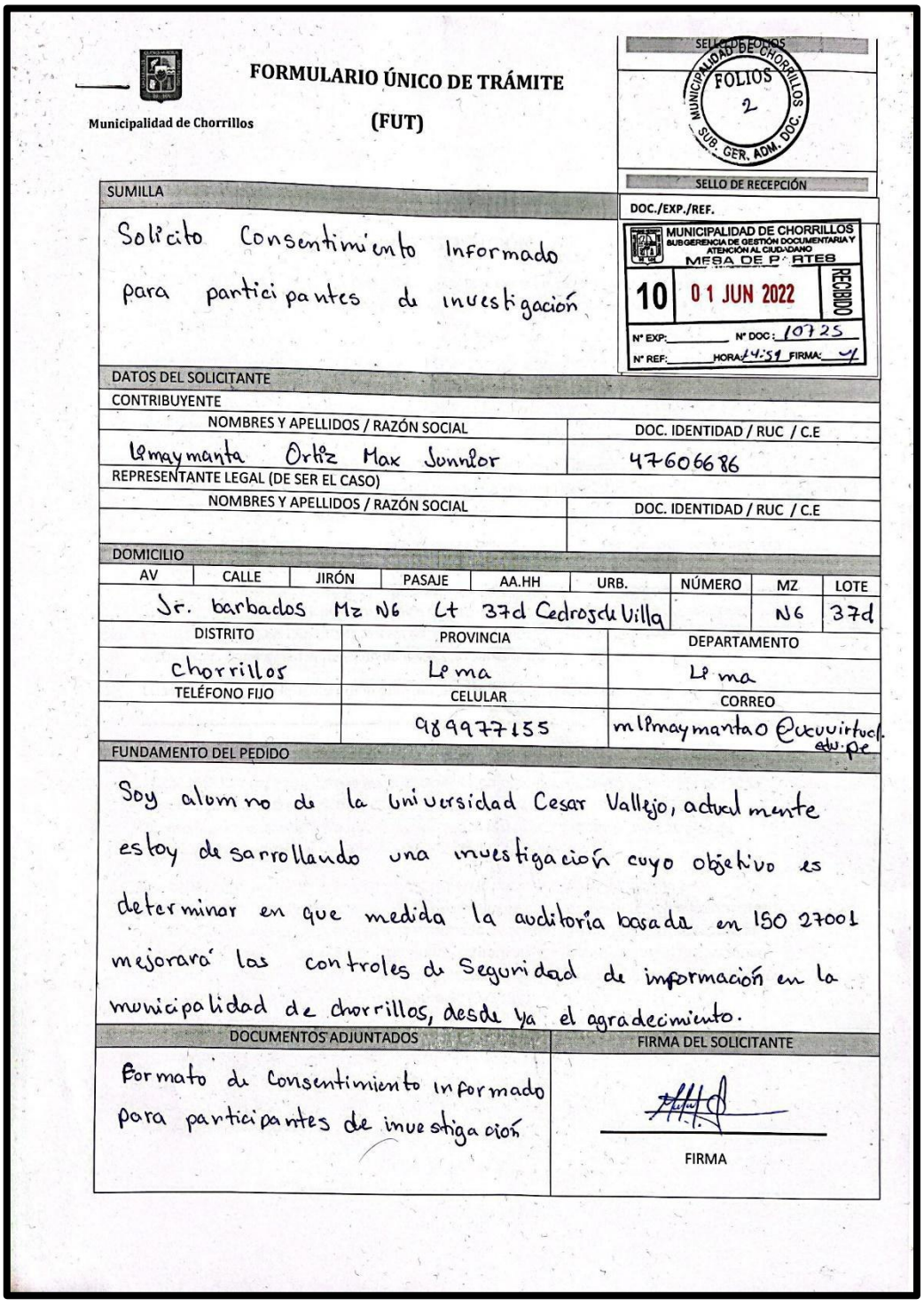
VELASCO, J., ULLAURI, R., PILICITA, L., JÁCOME, B., SAA, P. y MOSCOSO-ZEA, O., 2018. Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry., pp. 294-300. DOI 10.1109/INCISCOS.2018.00049.

ANEXOS

Anexo N°01: Conducta Responsable

Fuente: Concytec

Anexo N°02: Solicitud de Consentimiento informado para participantes de investigación de la Municipalidad de Chorrillos



Municipalidad de Chorrillos

FORMULARIO ÚNICO DE TRÁMITE

(FUT)

SELLO DE FOLIOS: MUNICIPALIDAD DE CHORRILLOS – FOLIOS 2 – SUB. GER. ADM. DOC.

SELLO DE RECEPCIÓN: MUNICIPALIDAD DE CHORRILLOS – SUBGERENCIA DE GESTIÓN DOCUMENTARIA Y ATENCIÓN AL CIUDADANO – MESA DE P. RTES – 10 – 01 JUN 2022 – RECIBIDO – N° EXP: ____ N° DOC: 10725 – N° REF: ____ HORA: 14:59 FIRMA: ____

SUMILLA

Solicito Consentimiento Informado para participantes de investigación

DOC./EXP./REF.

DATOS DEL SOLICITANTE

CONTRIBUYENTE

NOMBRES Y APELLIDOS / RAZÓN SOCIAL	DOC. IDENTIDAD / RUC / C.E
Lemaymanta Ortiz Max Junior	47606686

REPRESENTANTE LEGAL (DE SER EL CASO)

NOMBRES Y APELLIDOS / RAZÓN SOCIAL	DOC. IDENTIDAD / RUC / C.E

DOMICILIO

AV	CALLE	JIRÓN	PASAJE	AA.HH	URB.	NÚMERO	MZ	LOTE
Jr. barbados			Mz N6	Lt 37d	Cedros de Villa		N6	37d

DISTRITO	PROVINCIA	DEPARTAMENTO
Chorrillos	Lima	Lima
TELÉFONO FIJO	**CELULAR**	**CORREO**
	989977155	mlemaymanta0@ucvvirtual.edu.pe

FUNDAMENTO DEL PEDIDO

Soy alumno de la Universidad Cesar Vallejo, actualmente estoy desarrollando una investigación cuyo objetivo es determinar en que medida la auditoria basada en ISO 27001 mejorará los controles de Seguridad de información en la municipalidad de chorrillos, desde ya el agradecimiento.

DOCUMENTOS ADJUNTADOS	FIRMA DEL SOLICITANTE
Formato de Consentimiento informado para participantes de investigación	FIRMA

Fuente: Elaboración propia

Municipalidad de Chorrillos | chorrillos

CONSENTIMIENTO INFORMADO PARA PARTICIPANTES DE INVESTIGACIÓN

El propósito de esta ficha de consentimiento es proveer a los participantes en esta investigación con una clara explicación de la naturaleza de la misma, así como de su rol en ella como participantes.

La presente investigación es conducida por Max Junnior Limaymanta Ortiz de la Universidad Cesar Vallejo. La meta de este estudio es: Determinar en qué medida la auditoria basada en ISO 27001 mejorará los controles de seguridad de la información en la municipalidad de Chorrillos 2022.

Si usted accede a participar en este estudio, se le pedirá responder preguntas en una entrevista (o completar una encuesta, o lo que fuera según el caso). Esto tomará aproximadamente 60 minutos de su tiempo.

La participación es este estudio es estrictamente voluntaria. La información que se recoja será confidencial y no se usará para ningún otro propósito fuera de los de esta investigación. Si tiene alguna duda sobre este proyecto, puede hacer preguntas en cualquier momento durante su participación en él. Igualmente, puede retirarse del proyecto en cualquier momento sin que eso lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parece incómodas, tiene usted el derecho de hacérselo saber al investigador o de no responderlas.

Desde ya el agradecimiento por la oportunidad de poder realizar el estudio de investigación.

Yo el Sr **ERLAN HERNAN ROSPLIGIOSI AVILA**, Asesor de Tecnología de la Información de la Gerencia de Informática y Tecnología de la municipalidad de Chorrillos identificado con dni 10344083, acepto participar voluntariamente en esta investigación, conducida por el Sr Max Junnior Limaymanta Ortiz. He sido informado de que la meta de este estudio es: Determinar en qué medida la auditoria basada en ISO 27001 mejorará los controles de seguridad de la información en la municipalidad de Chorrillos 2022.

Reconozco que la información que yo provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de este estudio sin mi consentimiento. He sido informado de que puedo hacer preguntas sobre el proyecto en cualquier momento y que puedo retirarme del mismo cuando así lo decida, sin que esto acarree perjuicio alguno para mi persona. De tener preguntas sobre mi participación en este estudio, puedo contactar al número 989977155.

Entiendo que puedo pedir información sobre los resultados de este estudio cuando éste haya concluido. Para esto, puedo contactar al teléfono anteriormente mencionado.

MUNICIPALIDAD DE CHORRILLOS

Sr Erlan H Rospigliosi Avila
ASESOR EN TECNOLOGIA DE INFORMACIÓN

Fuente: Elaboración propia

Anexo N°03: Matriz de consistencia

Problema	Objetivo	Hipótesis	Metodología	Variables	Dimensiones	Indicadores	Instrumento
Problema general: ¿Cómo la auditoría basada en ISO 27001 mejorará los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana?	**Objetivo general:** Establecer si la auditoría basada en ISO 27001 mejora los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana.	**Hipótesis general:** La auditoría basada en ISO 27001 mejora los controles de seguridad de la información en la gerencia de informática y tecnología de una municipalidad peruana.	**Tipo de Investigación** El trabajo de investigación fue de tipo aplicable ya que la finalidad es la solución de un dificultad o método específico, enfocándose en la revisión e incorporación de experiencias para su puesta en marcha, fortaleciendo de este modo el desarrollo de la ciencia y la cultura.	**Variable Independiente:** Auditoría basada en la norma ISO 27001.	● Normatividad ● Infraestructura de TI ● Cultura de ciberseguridad	● Estado del dominio A5 de la seguridad de la información ● Estado del dominio A11 de la seguridad de la información ● Estado del dominio A7 de la seguridad de la información	● Ficha de observación ● Cuestionario
Problemas Específicos: ¿Cómo la auditoría basada en ISO 27001 mejorará la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de una municipalidad peruana? ¿Cómo la auditoria basada en ISO 27001 mejorará la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de una municipalidad peruana? ¿Cómo la auditoría basada en ISO 27001 mejorará la cultura de Ciberseguridad en la gerencia de informática y tecnología de una municipalidad peruana?	**Objetivos Específicos:** Establecer si la auditoria basada en ISO 27001, mejora la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de una municipalidad peruana. Establecer si la auditoría basada en ISO 27001, mejora la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de una municipalidad peruana. Establecer si la auditoria basada en ISO 27001, mejora la cultura de ciberseguridad en la gerencia de informática y tecnología de una municipalidad peruana.	**Hipótesis Específicas:** La auditoría basada en ISO 27001 mejora la generación de políticas de seguridad y su cumplimiento en la gerencia de informática y tecnología de una municipalidad peruana. La auditoría basada en ISO 27001 mejora la seguridad física de la infraestructura de TI en la gerencia de informática y tecnología de una municipalidad peruana. La auditoría basada en ISO 27001 mejora la cultura de ciberseguridad en la gerencia de informática y tecnología de una municipalidad peruana.	**Diseño de investigación:** El diseño de investigación fue experimental de su sub división preexperimental debido a que la investigación se realizó sin manejar intencionalmente a la variable independiente y se analizarán los eventos en su ámbito natural; Específicamente, nuestra muestra de estudio se analizará antes de la estimulación y luego se analizó la misma muestra de estudio.	**Variable Dependiente:** Controles de seguridad de la información.			

Anexo N°04: Operacionalización de variables

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES (SUB VARIABLES)	INDICADORES	ESCALA DE MEDICIÓN
VI: Auditoría basada en ISO 27001	Steve G. Watkins (2008) nos indica que la auditoría interna puede utilizarse para muchos fines, pero uno de los principales objetivos de la implantación de un régimen de auditoría interna es controlar la realización de los requerimientos del sistema de gestión y las prácticas de trabajo.	La auditoría mejorara los controles de seguridad de información en la municipalidad de Chorrillos ya que a través de este proceso asegurara la seguridad de información.			
VD: Controles de seguridad de la información	Casal (2022) manifiesta que el objetivo de los controles de seguridad informática es garantizar que todos los activos, sistemas, instalaciones, datos y ficheros asociados con la aplicación de la tecnología informática están resguardados respecto al acceso sin autorización, el daño y la utilización incorrecta que sea operable, seguro y protegido en todo momento.	Los controles de seguridad de la información de la municipalidad de Chorrillos mediante una auditoria basada en la norma ISO 27001.	● Normatividad ● Infraestructura de TI ● Cultura de Ciberseguridad	● Estado del dominio A5 de la seguridad de la información ● Estado del dominio A11 de la seguridad de la información ● Estado del dominio A7 de la seguridad de la información	● Ordinal ● Ordinal ● Ordinal

Anexo N°05: Listado de controles

ISO 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
   - 5.1 Directrices de la Dirección en seguridad de la información.
     - 5.1.1 Conjunto de políticas para la seguridad de la información.
     - 5.1.2 Revisión de las políticas para la seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
   - 6.1 Organización interna.
     - 6.1.1 Asignación de responsabilidades para la segur. de la información.
     - 6.1.2 Segregación de tareas.
     - 6.1.3 Contacto con las autoridades.
     - 6.1.4 Contacto con grupos de interés especial.
     - 6.1.5 Seguridad de la información en la gestión de proyectos.
   - 6.2 Dispositivos para movilidad y teletrabajo.
     - 6.2.1 Política de uso de dispositivos para movilidad.
     - 6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
   - 7.1 Antes de la contratación.
     - 7.1.1 Investigación de antecedentes.
     - 7.1.2 Términos y condiciones de contratación.
   - 7.2 Durante la contratación.
     - 7.2.1 Responsabilidades de gestión.
     - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
     - 7.2.3 Proceso disciplinario.
   - 7.3 Cese o cambio de puesto de trabajo.
     - 7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS.
   - 8.1 Responsabilidad sobre los activos.
     - 8.1.1 Inventario de activos.
     - 8.1.2 Propiedad de los activos.
     - 8.1.3 Uso aceptable de los activos.
     - 8.1.4 Devolución de activos.
   - 8.2 Clasificación de la información.
     - 8.2.1 Directrices de clasificación.
     - 8.2.2 Etiquetado y manipulado de la información.
     - 8.2.3 Manipulación de activos.
   - 8.3 Manejo de los soportes de almacenamiento.
     - 8.3.1 Gestión de soportes extraíbles.
     - 8.3.2 Eliminación de soportes.
     - 8.3.3 Soportes físicos en tránsito.
9. CONTROL DE ACCESOS.
   - 9.1 Requisitos de negocio para el control de accesos.
     - 9.1.1 Política de control de accesos.
     - 9.1.2 Control de acceso a las redes y servicios asociados.
   - 9.2 Gestión de acceso de usuario.
     - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
     - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
     - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
     - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
     - 9.2.5 Revisión de los derechos de acceso de los usuarios.
     - 9.2.6 Retirada o adaptación de los derechos de acceso
   - 9.3 Responsabilidades del usuario.
     - 9.3.1 Uso de información confidencial para la autenticación.
   - 9.4 Control de acceso a sistemas y aplicaciones.
     - 9.4.1 Restricción del acceso a la información.
     - 9.4.2 Procedimientos seguros de inicio de sesión.
     - 9.4.3 Gestión de contraseñas de usuario.
     - 9.4.4 Uso de herramientas de administración de sistemas.
     - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
    - 10.1 Controles criptográficos.
      - 10.1.1 Política de uso de los controles criptográficos.
      - 10.1.2 Gestión de claves.
11. SEGURIDAD FÍSICA Y AMBIENTAL.
    - 11.1 Áreas seguras.
      - 11.1.1 Perímetro de seguridad física.
      - 11.1.2 Controles físicos de entrada.
      - 11.1.3 Seguridad de oficinas, despachos y recursos.
      - 11.1.4 Protección contra las amenazas externas y ambientales.
      - 11.1.5 El trabajo en áreas seguras.
      - 11.1.6 Áreas de acceso público, carga y descarga.
    - 11.2 Seguridad de los equipos.
      - 11.2.1 Emplazamiento y protección de equipos.
      - 11.2.2 Instalaciones de suministro.
      - 11.2.3 Seguridad del cableado.
      - 11.2.4 Mantenimiento de los equipos.
      - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
      - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
      - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
      - 11.2.8 Equipo informático de usuario desatendido.
      - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.
    - 12.1 Responsabilidades y procedimientos de operación.
      - 12.1.1 Documentación de procedimientos de operación.
      - 12.1.2 Gestión de cambios.
      - 12.1.3 Gestión de capacidades.
      - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
    - 12.2 Protección contra código malicioso.
      - 12.2.1 Controles contra el código malicioso.
    - 12.3 Copias de seguridad.
      - 12.3.1 Copias de seguridad de la información.
    - 12.4 Registro de actividad y supervisión.
      - 12.4.1 Registro y gestión de eventos de actividad.
      - 12.4.2 Protección de los registros de información.
      - 12.4.3 Registros de actividad del administrador y operador del sistema.
      - 12.4.4 Sincronización de relojes.
    - 12.5 Control del software en explotación.
      - 12.5.1 Instalación del software en sistemas en producción.
    - 12.6 Gestión de la vulnerabilidad técnica.
      - 12.6.1 Gestión de las vulnerabilidades técnicas.
      - 12.6.2 Restricciones en la instalación de software.
    - 12.7 Consideraciones de las auditorías de los sistemas de información.
      - 12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.
    - 13.1 Gestión de la seguridad en las redes.
      - 13.1.1 Controles de red.
      - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
      - 13.1.3 Segregación de redes.
    - 13.2 Intercambio de información con partes externas.
      - 13.2.1 Políticas y procedimientos de intercambio de información.
      - 13.2.2 Acuerdos de intercambio.
      - 13.2.3 Mensajería electrónica.
      - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
    - 14.1 Requisitos de seguridad de los sistemas de información.
      - 14.1.1 Análisis y especificación de los requisitos de seguridad.
      - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
      - 14.1.3 Protección de las transacciones por redes telemáticas.
    - 14.2 Seguridad en los procesos de desarrollo y soporte.
      - 14.2.1 Política de desarrollo seguro de software.
      - 14.2.2 Procedimientos de control de cambios en los sistemas.
      - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
      - 14.2.4 Restricciones a los cambios en los paquetes de software.
      - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
      - 14.2.6 Seguridad en entornos de desarrollo.
      - 14.2.7 Externalización del desarrollo de software.
      - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
      - 14.2.9 Pruebas de aceptación.
    - 14.3 Datos de prueba.
      - 14.3.1 Protección de los datos utilizados en pruebas.
15. RELACIONES CON SUMINISTRADORES.
    - 15.1 Seguridad de la información en las relaciones con suministradores.
      - 15.1.1 Política de seguridad de la información para suministradores.
      - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
      - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
    - 15.2 Gestión de la prestación del servicio por suministradores.
      - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
      - 15.2.2 Gestión de cambios en los servicios prestados por terceros.
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
    - 16.1 Gestión de incidentes de seguridad de la información y mejoras.
      - 16.1.1 Responsabilidades y procedimientos.
      - 16.1.2 Notificación de los eventos de seguridad de la información.
      - 16.1.3 Notificación de puntos débiles de la seguridad.
      - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
      - 16.1.5 Respuesta a los incidentes de seguridad.
      - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
      - 16.1.7 Recopilación de evidencias.
17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
    - 17.1 Continuidad de la seguridad de la información.
      - 17.1.1 Planificación de la continuidad de la seguridad de la información.
      - 17.1.2 Implantación de la continuidad de la seguridad de la información.
      - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
    - 17.2 Redundancias.
      - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO.
    - 18.1 Cumplimiento de los requisitos legales y contractuales.
      - 18.1.1 Identificación de la legislación aplicable.
      - 18.1.2 Derechos de propiedad intelectual (DPI).
      - 18.1.3 Protección de los registros de la organización.
      - 18.1.4 Protección de datos y privacidad de la información personal.
      - 18.1.5 Regulación de los controles criptográficos.
    - 18.2 Revisiones de la seguridad de la información.
      - 18.2.1 Revisión independiente de la seguridad de la información.
      - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
      - 18.2.3 Comprobación del cumplimiento.

Anexo N°07: Modelo de Cuestionario

CUESTIONARIO SOBRE LOS CONTROLES DE SEGURIDAD DE INFORMACION BASADA EN LA NORMA INTERNACIONAL ISO 27001

El propósito de la herramienta es obtener datos para el trabajo de investigación titulado "Auditoria basada en la Norma ISO 27001 para la mejora de los Controles de Seguridad de la Información en la Gerencia de Informática y Tecnología en una Municipalidad Peruana"

Instrucciones:

- **Para desarrollar el siguiente cuestionario, usted debe leer cada pregunta y escoger una de las alternativas. Debe marcar con una "X" dentro del cuadro.**
- **La información proporcionada será confidencial.**
- **No dejar preguntas sin responder.**

Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.

ITEM	INDICADOR	PREGUNTA	Inicial	Repetible	Definido	Administrado	Optimizado
		Dimensión 2: Seguridad física y del entorno					
1	confidencialidad	¿Están todos los puntos de acceso externos adecuadamente protegidos contra el acceso no autorizado?					
2		¿Se monitorea los puntos de acceso con cámaras?					
3		¿Se utilizan sistemas de control de acceso adecuados (ej. Tarjetas de proximidad, biométrico, cerraduras de seguridad, monitorización CCTV, detección de intrusos)?					
4		¿Existe un registro de todas las entradas y salidas?					
5		¿Están los accesos (entrada y salida) de las instalaciones físicamente controlas (ej. Detectores de proximidad, CCTV)?					
6		¿Son proporcionados los controles de seguridad utilizados para salvaguardar las oficinas, salas e instalaciones con respecto a los riesgos?					
7		¿Existen protecciones contra el fuego, el humo, inundaciones, rayos, intrusos, vándalos, etc.?					
8		¿Existe un procedimiento de recuperación de desastres?					
9		¿Se verifican al final del día las oficinas, las salas de informática y otros lugares de trabajo?					
10		¿Se asegura que la información de carácter sensible permanece confidencial a personal autorizado?					
11		¿Se verifica que el material recibido coincide con un número de pedido autorizado?					
12		¿Se registran los detalles de la recepción de material según las políticas y procedimientos de adquisición, gestión de activos y seguridad?					
13		¿Las TIC y el equipo relacionado se encuentran en áreas adecuadamente protegidas?					
14		¿Las pantallas de los equipos de trabajo, las impresoras y los teclados están ubicados o protegidos para evitar la visualización no autorizada?					
15		¿Hay una red de suministro eléctrico redundante?					

Fuente: Elaboración propia

Anexo N°08: Solicitud de validación de instrumento de recojo de información

SOLICITUD: Validación de instrumento de Recojo de Información.

Sr. Dr. Daza Vergaray Alfredo

Yo **Limaymanta Ortiz Max Junnior** identificado con DNI N° **47606686** alumno de la Universidad Cesar Vallejo, a usted con el debido respeto me presento y le manifiesto:

Que siendo requisitos indispensables el recojo de datos necesarios para el proyecto de investigación que vengo elaborando que tiene como título "AUDITORIA BASADA EN ISO 27001 PARA LA MEJORA DE LOS CONTROLES DE SEGURIDAD DE INFORMACIÓN EN LA MUNICIPALIDAD DE CHORRILLOS 2022" solicito a Ud. se sirva validar el instrumento que le adjunto bajo los criterios académicos correspondientes. Para este efecto adjunto los siguientes documentos:

- Instrumento
- Matriz de operacionalización de variables, Por tanto:

A usted, ruego acceder mi petición.

Lima 08 de julio del 2022

Firma

Fuente: Elaboración propia

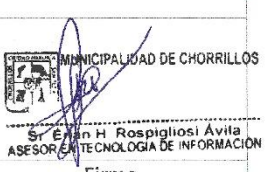
Anexo N°09: Revisión / Aprobación de la entrega de la Guía del Sistema de Gestión de seguridad de la Información.

APROBACIONES

Elabora por:	Revisado por:	Aprobado por:
Apellidos y nombres	Apellidos y nombres	Apellidos y nombres
Limaymanta Ortiz Max	Erlan Rospigliosi Avila	
	MUNICIPALIDAD DE CHORRILLOS Sr Erlan H Rospigliosi Avila ASESOR EN TECNOLOGÍA DE INFORMACIÓN	
Firma	Firma	Firma

Fuente: Elaboración propia

APROBACIONES

Elabora por:	Revisado por:	Aprobado por:
Apellidos y nombres	Apellidos y nombres	Apellidos y nombres
Limaymanta Ortiz Max Junnior		Erlan Rospigliosi Avila
		
Firma	Firma	Firma

Fuente: Elaboración propia

Anexo N°10: Aprobación de la Guía de Observación por parte del Encargado del área (PRE).

GUÍA DE OBSERVACIÓN

Docente a cargo: Dr. Daza Vergaray Alfredo	**Fecha:**
Observador: Limaymanta Ortiz Max Junnior	19/10/2022

A5. Políticas de seguridad de la información							
A5.1 Directrices de gestión de la seguridad de la información							
Aspecto a Evaluar/Observar	INEXISTENTE	INICIAL	REPETIBLE	DEFINIDO	ADMINISTRADO	OPTIMIZADO	**Observaciones**
A5.1.1 Políticas para la seguridad de la información							
¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Cómo se autorizan, comunican, comprenden y aceptan las políticas?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Están las políticas bien escritas, legible, razonable y viable?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.

Fuente: Elaboración propia

¿Incorporan controles adecuados y suficientes?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Cuán madura es la organización en esta área?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
A5.1.2 Revisión de las políticas para la seguridad de la información							
¿Todas las políticas tienen un formato y estilo consistentes?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Están todos al día, habiendo completado todas las revisiones debidas?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.
¿Se han vuelto a autorizar y se han distribuido?		X					Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de tener personal de alta calidad.

MUNICIPALIDAD DE CHORRILLOS
Sr. Franco Pospigliosi Ávila
ASESOR EN TECNOLOGÍA DE INFORMACIÓN

Firma del responsable del área

Firma del Experto

Fuente: Elaboración propia

Anexo N°11: Aprobación de la Guía de Observación por parte del Encargado del área (POST).

GUÍA DE OBSERVACIÓN

Docente a cargo: Dr. Daza Vergaray Alfredo	**Fecha:**
Observador: Limaymanta Ortiz Max Junnior	16/11/2022

A5. Políticas de seguridad de la información							
A5.1 Directrices de gestión de la seguridad de la información							
Aspecto a Evaluar/Observar	INEXISTENTE	INICIAL	REPETIBLE	DEFINIDO	ADMINISTRADO	OPTIMIZADO	**Observaciones**
A5.1.1 Políticas para la seguridad de la información							
¿Existe una clara evidencia de un marco / estructura / jerarquía global razonablemente diseñada y administrada?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Las políticas son razonablemente completas y cubren todos los riesgos de información y áreas de control relevantes?			X				La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios). La responsabilidad es individual. No hay formación.
¿Cómo se autorizan, comunican, comprenden y aceptan las políticas?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Están formalmente obligados a cumplir todos los trabajadores y, en su caso, sus empleadores?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Hay referencias cruzadas a buenas prácticas (como ISO27k, NIST SP800, CSC20 y otras normas y directrices relevantes)?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Están las políticas bien escritas, legible, razonable y viable?				X			El control se aplica conforme a un procedimiento documentado, pero no ha

Fuente: Elaboración propia

							sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Incorporan controles adecuados y suficientes?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Cubren todos los activos de información esenciales, sistemas, servicios, etc.?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Cuán madura es la organización en esta área?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
A5.1.2 Revisión de las políticas para la seguridad de la información							
¿Todas las políticas tienen un formato y estilo consistentes?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Están todos al día, habiendo completado todas las revisiones debidas?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.
¿Se han vuelto a autorizar y se han distribuido?				X			El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el responsable de Seguridad ni el Comité de Dirección.

MUNICIPALIDAD DE CHORRILLOS
Sr. Érlan H. Rospigliosi Ávila
ASESOR EN TECNOLOGÍA DE INFORMACIÓN

Firma del responsable del área

Firma del Experto

Fuente: Elaboración propia

Anexo N°12: Aprobación de la recolección de datos por parte del Encargado del área.

CARTA DE ACEPTACIÓN DE RECOLECCIÓN DE DATOS

Yo el Sr. ERLAN HERNAN ROSPIGLIOSI AVILA, asesor de Tecnología de la Información de la Gerencia de Informática y Tecnología de la municipalidad de Chorrillos identificado con DNI 10344083, con el fin de informar que el Sr. Max Junnior Limaymanta Ortiz con DNI 47606686, ha realizado exitosamente el proceso de recolección de datos utilizando un Cuestionario al personal del área de Gerencia de Informática y Tecnología.

Asimismo, se recibió afiches informativos referentes a las políticas de seguridad de la Información y se colocaron en espacios estratégicos para difundir el mensaje.

MUNICIPALIDAD DE CHORRILLOS
Sr. Erlan H. Rospigliosi Avila
ASESOR EN TECNOLOGIA DE INFORMACIÓN

Lima, 16 de noviembre del 2022.

Fuente: Elaboración propia

Anexo N°13: Estado de controles del anexo A de la norma ISO 27001

Estado	Significado
? Desconocido	No ha sido verificado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.

Fuente: ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap analysis) workbook disponible en:

https://www.iso27001security.com/

Anexo N°14: Guía para el Sistema de gestión de seguridad de la información – SGSI

Fuente: Elaboración propia

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Declaratoria de Autenticidad del Asesor

Yo, DAZA VERGARAY ALFREDO, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Auditoria basada en la Norma ISO 27001 para la mejora de los Controles de Seguridad de la Información en la Gerencia de Informática y Tecnología en una Municipalidad Peruana.", cuyo autor es LIMAYMANTA ORTIZ MAX JUNNIOR, constato que la investigación tiene un índice de similitud de 25.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 18 de Diciembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
DAZA VERGARAY ALFREDO **DNI:** 40466240 **ORCID:** 0000-0002-2259-1070	Firmado electrónicamente por: ADAZAVE el 18-12-2022 22:11:41

Código documento Trilce: TRI - 0494529

INVESTIGA UCV