ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Aplicación de la Norma Técnica Peruana ISO - IEC 27001 en la seguridad informática de la Oficina General de Tecnologías de la SUCAMEC Lima 2018

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con Mención en Tecnologías de la Información

AUTOR:

Sacravilca Narciso, Dante Gonzalo (orcid.org/0009-0003-8042-8145)

ASESORES:

Dra. Sihuay Maravi, Norma Agripina (orcid.org/0000-0002-4023-2688)

Dr. Sánchez Ortega, Jaime Agustín (orcid.org/0000-0002-2916-7213)

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

LIMA – PERÚ

2018

Dedicatoria

A nuestro Señor todopoderoso que día a día me da las fuerzas y los ánimos para seguir superándome y crecer en todas las áreas de mi vida, a mis padres que se encuentran en la presencia de Dios, quienes con su sabiduría me dieron el consejo y guía en mi proyectos de vida y a mi hijo Alejandro Gabriel fruto de mi experiencia terrenal de vida.

Agradecimiento

Al Dr. Jaime Agustín Sánchez Ortega, por su meritorio soporte y guía, a los maestros docentes de nuestra prestigiosa Alma Mater Universidad “Cesar Vallejo”, a mis colegas en general, quienes con sus consejos, sabiduría y experiencia compartieron sus conocimientos para el desarrollo del presente trabajo de investigación.

Declaratoria de autenticidad del asesor

UNIVERSIDAD CÉSAR VALLEJO

Declaratoria de autenticidad del asesor

Yo, Norma Agripina Sihuay Maravi , docente de la Escuela de Posgrado de la Universidad César Vallejo filial Lima Norte asesor de la tesis titulada: "APLICACIÓN DE LA NORMA TÉCNICA PERUANA ISO - IEC 27001 EN LA SEGURIDAD INFORMÁTICA DE LA OFICINA GENERAL DE TECNOLOGÍAS DE LA SUCAMEC LIMA 2018" del estudiante SACRAVILCA NARCISO, DANTE GONZALO, constato que la investigación tiene un índice de similitud de **14%** 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, 9 de enero del 2024

Apellidos y Nombres del Asesor: Dra. Norma Agripina Sihuay Maravi	
DNI: 19911015	Firma:
ORCID: 0000-0002-4023-2688	

Declaratoria de originalidad del autor/ autores

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Declaratoria de Originalidad del Autor

Yo, SACRAVILCA NARCISO DANTE GONZALO estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN INGENIERIA DE SISTEMAS CON MENCION EN TECNOLOGIAS DE LA INFORMACION de la UNIVERSIDAD CÉSAR VALLEJO SAC – LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: " Aplicación de la Norma Técnica Peruana ISO - IEC 27001 en la seguridad informática de la Oficina General de Tecnologías de la SUCAMEC Lima 2018", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda citatextual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro gradoacadémico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, nicopiados.

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

SACRAVILCA NARCISO DANTE GONZALO

Índice de Contenidos

Índice de tablas

Índice de figuras

Resumen

El presente trabajo de tesis consiste en determinar en qué medida la aplicación de la NTP ISO/IEC 27001 influye en la seguridad informática en la Oficina General de Tecnologías - OGT de SUCAMEC, 2018, se utilizarán las recomendaciones que sugieren la Norma Técnica Peruana NTP ISO/IEC 27001. Manual de Políticas de Seguridad Informática - Buenas Prácticas, bibliografía especializada y otros documentos referentes a la seguridad informática.

El tipo de investigación fue aplicada y con un diseño experimental del tipo pre experimental pre test y post test debido que permitió medir antes y después de la aplicación del tratamiento, la población estuvo conformada por 45 personas conformada por la Oficina General de Tecnologías - OGT de SUCAMEC. La técnica utilizada fue la encuesta a través de un cuestionario para cotejar información el cual se validó con el juicio de expertos. El análisis de los datos recolectados, se realizó con el apoyo de la herramienta de software SPSS, lo cual determinó la existencia de diferencias significativas entre los datos del pre test y post test.

Luego de emplear el instrumento y ejecutar el análisis estadístico se evidencio un aumento significativo en los indicadores evaluados: control de accesos se obtuvo una mejora de 39,1%, en seguridad de la operatividad un aumento del 102,1% en gestión de incidentes en la seguridad de la información un 85,5%.

Palabras clave: Políticas de seguridad informática, tecnologías de información y comunicación, norma NTP ISO/IEC 27001.

Abstract

The present thesis work is to determine the extent to which the application of NTP ISO / IEC 27001 influences computer security in the General Office of Technologies

-OGT of SUCAMEC, 2018, will use the recommendations that suggest the Peruvian Technical Standard NTP ISO / IEC 27001. Manual of Information Security Policies

-Good Practices, specialized bibliography and other documents related to computer security.

The type of research was applied and with an experimental design of the pre-experimental type, pre-test and post-test, which allowed to measure before and after the application of the treatment, the population consisted of 45 people conformed by the General Office of Technologies - OGT de SUCAMEC. The technique used was the survey through a questionnaire to collate information which was validated with expert judgment. The analysis of the data collected was carried out with the support of the SPSS software tool, which determined the existence of significant differences between the pre-test and post-test data.

After using the instrument and executing the statistical analysis, a significant increase in the evaluated indicators was evidenced: access control obtained an improvement of 39.1%, in safety of the operation an increase of 102.1% in incident management in information security 85.5%.

Keywords: IT security policies, information and communication technologies, NTP ISO / IEC 27001 standard.

I. INTRODUCCIÓN

Dado que la información es el pilar principal para mejorar cualquier tarea de distribución, la seguridad informática en el sector estatal internacional así como del sector particular es un prisma particularmente importante. En este sentido, cualquier pérdida de servicios de consultoría puede resultar en rechazos importantes de la gestión relevante, las condiciones financieras o la situación actual. Estas frustraciones por el deterioro de los informes son cosa de veteranos del sector público. Por lo tanto, las universidades del sector público deberían realizar actividades con la mayor frecuencia posible para compensar los errores causados por las obligaciones de información.

Con este fin, las organizaciones aplican SGSI, resaltando la relevancia en el informe del sector estatal en Chile. Los objetivos principales son asegurar la confidencialidad de los datos consultados por individuos en el ámbito público, preservar su integridad, asegurar su universalidad y precisión, y garantizar la disponibilidad de esa información a las autoridades competentes en el momento requerido.

Evaluar la seguridad informática en el ámbito público es un paso inicial antes de llevar a cabo la instalación del SGSI en la entidad. Mediante este informe, se pretende determinar el estado de la organización en la seguridad informática, aprender cómo se desenvuelven las tareas actuales, establecer un punto de partida y, a partir de ello, implementar de manera efectiva el SGSI.

Este informe es importante por su capacidad para: examinar el estado actual y proponer las acciones y niveles de control requeridos para respaldar la seguridad informática. Además, permite evaluar el desarrollo del SGSI implementado con el fin de identificar y establecer las correcciones necesarias.

Principalmente, con la llegada de la versión actualizada de la norma ISO 27001:2013, este informe es fundamental para evaluar la diferencia existente entre los requisitos ya implementados en la organización y aquellos que aún deben ser incorporados; esta discrepancia se conoce comúnmente como análisis de brechas (GAP).

La evaluación de la seguridad informática en Chile debe ser llevada a cabo en colaboración con todos los participantes de los distintos procesos, y su divulgación debe extenderse a todas las partes implicadas.

Fundamentalmente, cuando se trata de verificar este diagnóstico en el cuidado informático inapelable en la ejecución del SGSI por la organización, señala varias opciones: evaluación del riesgo, análisis GAP de la actual situación de la Seguridad informática frente a la ISO 27001:2013, análisis GAP para calcular el cumplimiento de controles respecto a ISO 27002:2013, identificar el nivel de crecimiento de la seguridad de nuestro SGSI, análisis efectuado por expertos en la institución, auditorías integrales que verifiquen la situación de la seguridad informática que posee la institución; por último, el diagnóstico basado en el nivel de cumplimiento de los requerimientos concretos situados por ciertas instituciones públicas.

Según el estudio realizado por ESET, a nivel de Latinoamérica el 60% de las instituciones privadas y estatales señala que el mayor incidente a la hora de atentar contra la información se concentra en el código dañino. Además, muestra un “Reporte de Seguridad”, el cual presento la seguridad y su situación en las entidades tanto privadas como estatales en Latinoamérica. Por lo que, este reporte nos muestra que el 20% de las instituciones regionales han recibido atentados en el último año donde se encontró que el daño por lo común es el ataque fraudulento sumado del ingreso no permitido a las instituciones privadas y estatales.

Podemos agregar, que para entender a las entidades y la situación por la que atraviesan, se plasmarán muestras para poder responder lo siguiente: En primer lugar, se testifica la prevención de los grupos responsables del cuidado de la información, se cuestionó por la frecuencia con que se presentaban los ataques el último año, y todo lo que permitió analizar si las inquietudes se vincularon con los desafíos que se trazan las instituciones privadas y estatales o son muy desiguales. En segundo lugar, se vincula con los ciberataques en tiempo real los atentados ocurridos en el lapso de análisis. Además, es importante entender que incidencia exacta fue la causante y esto nos permitirá entender si el tratamiento usado está acorde a las necesidades. Por tanto, en esta sección se muestran cuáles son los atentados frecuentes por ciber-delincuentes, siendo el ingreso no permitido,

proliferación de malware y atentados en tiempo real en la anulación del acceso a internet. En tercer lugar, los procedimientos ejecutados por las instituciones privadas y estatales necesitan protección de su información porque fomenta garantizar el cuidado de su información utilizando ítems que involucran la tecnología. Por último, en cuarto lugar, es observar su evolución en los últimos cinco años en las incidencias y casos para su detención. Entre lo más relevante se observa la infección por código inadecuado que según los reportes ha crecido un 44%; el ingreso no permitido a las cuentas de sistemas presenta un crecimiento en un 13% en el año 2013 y en un 44% en el año 2014, pero la supervisión para el control de incidencias fue lo que no creció, respecto a un 20% en las instituciones privadas y estatales.

En el presente reporte ESET señala que las instituciones privadas y estatales conocerán la situación real con respecto de la seguridad de su información, comparar las acciones cercana de los incidentes presentados y alinear su táctica de seguridad con lo que está ocurriendo en la región.

En esta situación, las instituciones privadas y estatales adoptan posturas en igualdad con sus políticas de seguridad nacional, antelándose a través del uso de herramientas los posibles ataques, siempre apostando por la enseñanza como un mecanismo de seguridad y siendo conscientes que deberíamos estar cada vez más interconectados, sentirnos seguros sobre nuestra información es una necesidad importante de ejecutar en entornos privados e instituciones del estado.

En la actualidad, en Perú, SUCAMEC cuenta con un equipo de 45 personas en la Oficina de Gestión de Tecnologías (OGT), donde se han identificado varias deficiencias. Entre ellas se destaca el acceso inadecuado al sistema por parte de individuos con privilegios mínimos de información, lo que expone a riesgos la confidencialidad de la información dentro de la institución SUCAMEC. Además, la OGT no tiene firewalls físicos para proteger la información de ataques cibernéticos externos, esto seguiría siendo perjudicial en la disponibilidad informática para tomar decisiones. Por otro lado, el personal demanda seguridad en el funcionamiento y efectividad del sistema para prevenir perdidas de datos en la información afectando la integridad de la información. Por lo que, si esta situación continúa la OGT podría desencadenar un incidente grave presentando como consecuencia la falta de

capacitación al personal que trabaja en esta área tecnológica. En resumen, el propósito de esta investigación en la OGT es implementar las mejores prácticas de seguridad informática referidas por el estándar ISO IEC 27001, la cual se basa en el estándar ISO 27001. El propósito es mejorar pilares de la seguridad informática y, como consecuencia, fortalecer las operaciones de la OGT.

La justificación metodológica siguió el método científico de utilizar un cuestionario como herramienta de recogida de datos, validar el cuestionario y determinar su viabilidad. La aplicación de este enfoque posibilitará que otras personas aborden sus desafíos de manera similar. Por ende, a través de este estudio, se evaluará el efecto considerable de implementar NTP ISO IEC 27001 a la seguridad informática de la OGT de la SUCAMEC. en el orden en que es utilizada por otras organizaciones del mismo rubro. La legitimidad teórica implica la creación de un procedimiento informativo por parte de un individuo o grupo, que se puede interpretar como la elección de las opciones más óptimas. Con los adelantos de la tecnología informática, hemos desarrollado habilidades avanzadas para influir en las decisiones. Sin embargo, es esencial sintetizar y emplear diversas fuentes de investigación para respaldar una toma de decisiones genuina. De igual manera, la validación social cumple con la sugerencia de asignar recursos para respaldar la mejora de la excelencia en las decisiones mediante métricas recomendadas que permiten conocer y comprender la situación actual de la seguridad TI en la OGT. Esto la convierte en una entidad gubernamental mediante la cual se pueden lograr progresos significativos.

Para la investigación el problema general que se trató resolver es, ¿En qué medida la aplicación de la NTP ISO/IEC 27001 Influye en la seguridad informática de la OGTIC de SUCAMEC?

Partiendo del problema general se tuvo los siguientes problemas específicos: 1. ¿En qué medida la aplicación de la NTP ISO/IEC 27001 influye en la confidencialidad de la seguridad informática en la OGTIC de SUCAMEC? 2. ¿En qué medida la aplicación de la NTP ISO/IEC 27001 influye en la integridad de la seguridad informática en la OGTIC de SUCAMEC? 3. ¿En qué medida la aplicación del modelo NTP ISO/IEC 27001 influye en la disponibilidad de la seguridad informática en la OGTIC de SUCAMEC?

En esta investigación, el principal objetivo Determinar en qué medida la aplicación del modelo NTP ISO/IEC 27001 mejora la seguridad informática en la OGTIC de SUCAMEC. A su vez partiendo del problema general se tuvo los siguientes problemas que se especifican a continuación: 1. Determinar la influencia de la NTP ISO/IEC 27001 en la confidencialidad de la seguridad informática en la OGTIC de SUCAMEC. 2. Determinar la influencia de la NTP ISO/IEC 27001 en la integridad de la seguridad informática en la OGTIC de SUCAMEC. 3. Determinar la influencia de la NTP ISO/IEC 27001 en la disponibilidad de la seguridad informática en la OGTIC de SUCAMEC. Para la investigación la hipótesis general es: La aplicación de la NTP ISO/IEC 27001 influye de manera significativa en la seguridad informática en la OGTIC de SUCAMEC. Las hipótesis específicas planteadas son: 1. La aplicación de la NTP ISO/IEC 27001 influye de manera significativa en la confidencialidad de la seguridad informática en la OGTIC de SUCAMEC. 2. La aplicación del modelo NTP ISO/IEC 27001 influye de manera significativa en la integridad de la seguridad informática en la OGTIC de SUCAMEC. 3. La aplicación del modelo NTP ISO/IEC 27001 influye de manera significativa en la disponibilidad de la seguridad informática en la OGTIC de SUCAMEC.

II. MARCO TEORICO

En el ámbito internacional, según el trabajo de investigación realizado por Ramírez (2020) con el título "Diseño de un SGSI para los procesos de software y soporte de la empresa ALFCOM S.A", se basa en el estándar ISO IEC 27001:2013. Este diseño representa un esfuerzo dirigido a adquirir especialización en seguridad informática. Basado en una investigación cuantitativa no experimental, con métodos descriptivos; Aplicada a una muestra de empleados municipales, se utilizó una encuesta basada en cuestionarios para recolectar datos. Concluyendo que: el sistema de seguridad informática debe priorizarse en toda entidad que dirija o controle información personal de cada individuo salvaguardando su integridad, implementar este sistema permite que no sean vulnerados ni expuestos información por la empresa y que por lo contrario esto debe ser implementado desde la gerencia de toda empresa, siempre proyectándose a reducir las vulnerabilidades.

Peñafiel (2019) en el estudio titulado Diseño de un modelo para el establecimiento de un SGSI en un entorno de computación en la Nube, aplicando las normas ISO 27001:2013. Tesis para la licenciatura en Sistemas en Ecuador, cuyo propósito es: “Diseñar un modelo en seguridad informática para la implementación de un SGSI según los estándares ISO IEC 27001:2013 en un entorno: computación en la Nube” basada en un estudio cuantitativo, experimental porque se hace uso de un previo experimento respecto a las variables del estudio ISO27001. Concluyendo: que a lo largo del tiempo las organizaciones públicas y privadas deciden invertir en los recursos de seguridad informática de manera continua, capacitando a los usuarios sobre la importancia de plasmar dicha plataforma. Por lo que, la seguridad es una alteración persistente en las empresas que debido a los cambios establecidos deciden reemplazar los métodos tradicionales a un espacio Cloud Computing que promueve mayor seguridad, eficiencia y protección respecto a la información que posee.

Según Calder y Watkins (2019) sostienen que las organizaciones, en su mayoría consideran presupuesto para invertir sistemas de información para posicionarse en el mercado, buscar la excelencia operacional, incursionar en nuevos modelos de negocios, cercanía con los clientes y proveedores, ventaja

competitiva frente a sus competidores; todo ello está basado en el adecuado manejo de la información que ayude a tomar decisiones estratégicamente.

Andrade y Chávez (2018) a través de un estudio enfocado en la mejora de los procesos a través de la norma ISO 27001 determinó que, ante factores de riesgo existente, los planes de mejora garantizan los aspectos de integridad, disponibilidad y accesibilidad.

De acuerdo a lo descrito en líneas anteriores, la información física y digital desempeña un rol importante ya que es el activo clave de toda organización. Si una empresa no administra adecuadamente su información, estará altamente vulnerable a los riesgos lo que podría afectar la continuidad del negocio. Por ello, es importante que se establezca mecanismos de seguridad para proteger la información (Gómez y Católico, 2010).

Prada y Ortiz (2022) en su investigación titulada Diseño de un SGSI para el área de TIC del hospital San Vicente de Paúl. Tesis para obtener el grado en ciberseguridad, Ibagué – Colombia. Que tuvo como objetivo: “Diseñar un SGSI basado en el estándar ISO IEC 27001:2013 que gestione los tres pilares de la información del área de TIC en el Hospital”. Basada en un estudio descriptivo con un enfoque cualitativo, aplicada en una recolección de información se utilizará entrevistas y cuestionarios con el encargado de cada área hospitalaria. Concluyendo que: existe vulnerabilidad con respecto a las amenazas latentes que presenta el centro hospitalario en base a la seguridad de información por lo que se debe buscar nuevas políticas con el fin de anteponer la importancia que amerita, un estudio de análisis de seguridad informática sería de gran efectividad y eficiencia respecto a diversos procesos tanto asistenciales como administrativos.

Dentro del contexto nacional, se tiene que, Villadeza y Condor (2022) en su investigación titulada Estudio sobre el SGSI sustentado en el estándar ISO 27001:2014 y lograr recibir el grado de profesional en sistemas, por la Universidad Nacional Hermilio Valdizán, Perú. Que tuvo como objetivo: "Sugerir la creación del SGSI fundamentado en el estándar ISO IEC 27001:2014, con el propósito de consolidar la seguridad informática en la Municipalidad." basado en una investigación cuantitativa no experimental, con métodos descriptivos; aplicado a una muestra de empleados municipales, se utilizó una encuesta basada en

cuestionarios para recopilar datos. Concluyendo que: es significativo la gran relevancia respecto a las diferentes carencias sistemáticas que existe respecto a la seguridad en la entidad municipal, en donde el cuidado debe ser mucho mayor ya que están expuestos diversos documentos importantes, la importancia de cada servicio estará expuesta dependiendo de la protección de la información.

Monteza (2019) en el estudio titulado: SGSI sustentado en el estándar ISO 27001:2013 en el Municipio de El Agustino para recibir el grado de profesional en redes y comunicaciones, por la UPC Perú cuyo objetivo: “Diseñar el SGSI sustentado en el estándar ISO 27001:2013 para el respaldo satisfactorio de los activos informáticos del proceso fiscalizador tributario.” Basada en un estudio no experimental, cuantitativo con métodos descriptivos, aplicados a una muestra de personal que labora en la municipalidad, para la toma de datos se hizo uso de una encuesta basada en cuestionarios. Concluyendo: las medidas de seguridad en la entidad municipal son deficiente y aún le falta mucho para lograr una seguridad adecuada, ya que es un tema que no es priorizado y tampoco se observa que los funcionarios tomen con precaución o descontento la ineficiencia de la seguridad informática. Por lo que, el elaborar un sistema que en base al estándar ISO 27001:2013 proteja adecuadamente la información de los diversos procesos tributarios es lo esperado.

Santos (2016) realizo un estudio relacionado con el entorno de riesgos en una empresa consultora de software, para ello empleo la metodología Margerit; el investigador concluyó que la empresa exitosa depende de insumos diversos, entre ellos la elaboración de dispositivos apropiados y que a su vez cumplan con las exigencias del ISO 27001.

Por su parte Talavera (2015) y Vilca (2017) diseñaron modelos de gestión de la seguridad en los que se aplicaron la metodología de análisis de riesgos, la metodología de valoración de activos teniendo como conclusión que las implementaciones de los sistemas de gestión de la seguridad de la información determinan los riesgos al interior de una empresa.

Asqui y Torres (2023) en su investigación titulada ISO 27001 para mejorar la seguridad informática en una institución educativa. Tesis para graduarse en sistemas e informática, Perú. Que tuvo como objetivo:” Demostrar cómo la ISO

27001 mejora la seguridad informática en una institución educativa.” Basada en un estudio cuantitativo, experimental porque se hace uso de un previo experimento respecto a las variables del estudio ISO27001 con el fin de mejorar la seguridad informática, para la recolección de datos comprende 22 controles en base a la observación antes, durante y después en base a la Norma ISO 27001. Concluyendo que: implementar la ISO27001 mejora la seguridad de información educativa un 61.6%, respecto a sus cifras se indica que las incidencias eran hasta de 209 y luego de implementar el sistema de seguridad esto disminuyo a una incidencia de 39.

Un paradigma es un modelo o teoría que explica un efecto físico. El significado del modelo científico utilizado actualmente en la observación de la ciencia fue dado por Thomas Kuhn (1975) para dar a conocer las “revoluciones de la ciencia”. Según Karl Popper, las exposiciones terminarán al descubrir una teoría novedosa para rechazar la antigua, y que será la primera piedra para su desarrollo. Para Kuhn, la motivación era naturalmente un “revolución del paradigma” para la elucidación de fenómenos naturales; La novedad teórica no significa necesariamente una distorsión de la anterior, puede ser una posibilidad, un nuevo paradigma o un argumento arquetípico, un nuevo paradigma.

En teorías referentes a la investigación se revisó la siguiente literatura:
Históricamente, la seguridad informática solía ser concebida como la disciplina que abarca diversas normas, aplicaciones y mecanismos destinados a garantizar la seguridad informática del sistema y de sus usuarios. El extenso y perjudicial ataque cibernético perpetrado por Rusia contra Estonia en 2007, y la proximidad incluso por parte de China, a la división de Defensa ubicada en la Intranet del Jet Propulsion Laboratory - NASA, fueron incidentes que llevaron a una revisión del alcance y los objetivos de la seguridad informática.

El experto Hernán Montejano enfatiza que la noción de seguridad informática ha evolucionado para convertirse en un tema de extrema sensibilidad y de importancia crítica en el ámbito de la Defensa. En este sentido, ha superado el ámbito de un sistema informático y sus usuarios. La seguridad informática constituye el aspecto más delicado de los sistemas financieros de una nación, así como de la infraestructura industrial, los sistemas de energía y la seguridad social. Durante los conflictos entre naciones, se evidenció de inmediato la vulnerabilidad

del sistema financiero de un país mediante la violación de las medidas tecnológicas estándar, la destrucción de puntos críticos mediante ataques cibernéticos y el acceso perjudicial a información secreta y altamente relevante para la defensa.

La transformación fundamental en el ámbito de la seguridad informática radica en la necesidad prácticamente imperativa para todos los países de adquirir habilidades para identificar la entrada de agentes maliciosos especializados, como los gusanos y Caballos de Troya, en las instalaciones gubernamentales más sensibles. Esto implica la capacidad de identificar estos programas con el fin de aislarlos, reconstruir su código fuente mediante conocimientos y técnicas de reingeniería, así como detectar sus fuentes de origen y neutralizar sus capacidades.

En consecuencia, tanto en instituciones académicas de Brasil como de Argentina, se desarrollaron capacitaciones basados en los paradigmas nuevos en seguridad informática. Dentro del contexto de los actuales programas de colaboración, se generan efectos sinérgicos altamente eficaces. Por lo tanto, sería altamente beneficioso que los gobiernos de Brasil y Argentina brinden un mayor respaldo a estos programas de contribución. Cabe destacar que los desafíos a enfrentar pueden ser categorizados como desafíos de gestión gubernamental y tecnológicos.

La seguridad informática y su relevancia se pueden abordar inicialmente mediante una definición oficial como la que se establece en la documentación ISO 27000. Según esta definición, un SGSI comprende los procedimientos y recursos que son gestionadas por una organización con el propósito de resguardar su información. Asimismo, se alinea con los niveles predeterminados de tolerancia a riesgos establecidos por la organización con el fin de gestionar de manera efectiva los riesgos y salvaguardar los activos informáticos y la implementación controlada para asegurar dichos activos, según sea necesario, son elementos fundamentales para la exitosa implementación de un SGSI.

En esta perspectiva, los conceptos de "Información" y "Seguridad Informática" se conceptualizan de manera bastante exhaustiva. La información se presenta como un activo almacenado en diversas formas, incluyendo el conocimiento poseído por los empleados. La naturaleza de la información está

vinculada a las tecnologías utilizadas en la organización, por lo tanto, las TIC se convierten en un factor crucial.

La seguridad de la información comprende tres aspectos, denominados por el estándar ISO IEC 27000:2014 como "dimensiones", que son la Confidencialidad, Disponibilidad e Integridad.

Conforme a los redactores del estándar ISO 27001, "la seguridad informática abarca la implementación y su manejo pertinentes que aborden una amplia variedad de amenazas. El propósito es lograr el éxito comercial sostenido, garantizar la continuidad y minimizar los incidentes relacionados con la seguridad informática". La seguridad informática se despliega a través de la ejecución de controles escogidos según la necesidad de los riesgos adoptados y administrados por un SGSI. Estos controles comprenden políticas, procedimientos, estructuras organizativas, software y hardware destinados a salvaguardar los activos de información identificados. Es fundamental especificar, implementar, observar, supervisar y optimizar los controles según la necesidad para tener éxito en los objetivos específicos de la seguridad informática y comercial de la organización, así los controles pertinentes de seguridad de la información se integran de manera fluida con los procesos comerciales de la entidad.

Podemos incorporar el hecho de que los estándares guían el estándar de la seguridad informática en nuestro enfoque de procedimientos y gestión. Las actividades incluyen las acciones, formas, prácticas y controles de la gestión de recursos que se extienden desde un individuo hasta grupos organizados de personas responsables de la S.I. Proteger la información mientras se logran los objetivos planteados.

La instalación de un SGSI permite a una organización cumplir con los requisitos establecidos por los clientes y otras partes interesadas. Además, posibilita la optimización de los planes y actividades organizacionales, el logro de las metas específicas en materia de S.I., cumplir con regulaciones, leyes y normativas sectoriales, además de gestionar eficientemente toda información para facilitar la continua mejora y los lineamientos con los objetivos actuales de la entidad.

En todas las situaciones, la implementación de un enfoque centrado en procesos habilita a las organizaciones para perseguir los objetivos de la seguridad informática sin estar atadas a tecnologías y herramientas particulares, mediante la descripción de cualquier actividad mediante la transformación de entradas en productos mediante el uso de conjuntos de actividades. Esas actividades pueden estar relacionadas entre sí para interactuar entre ellas creando un proceso. Luego, muchos de estos procesos pueden interactuar directamente entre sí en condiciones planificadas y controladas a través de insumos y productos, creando un sistema de procesos y permitiendo a la organización definir y aplicar su enfoque de proceso a sus propios procedimientos de SGSI.

En todos los casos, el SGSI juega un papel vital en la seguridad informática de una organización y las vulnerabilidades relacionada con ataques debido a incidentes humanos, físicos y tecnológicos. Esto incluye todas las formas de información en una organización. Por lo tanto, la adopción del SGSI se considera una decisión estratégica para una organización. Por ende, debe ser incorporada y planificada según los requisitos específicos, lo que implica la creación e implementación de un SGSI adaptado a las características particulares de la entidad que debe basarse en la estructura organizativa y los procesos comerciales establecidos y también en los requisitos de seguridad de todos los interesados .

Es importante señalar que el concepto subyacente del SGSI no solo implica la instalación del sistema, sino también la supervisión, el mantenimiento y la mejora constante del SGSI. Este proceso se realiza con la finalidad de garantizar que el SGSI implementado resguarde de manera eficaz y constante los activos informáticos de la entidad. Por lo tanto, existe una necesidad instantánea de reconocer la información y sus requerimientos, la evaluación de riesgos y beneficios relacionados, para señalar e implementar controles relevantes para administrar los riesgos reconocidos, y luego monitorear y perfeccionar los controles del sistema conforme a las necesidades empresariales y los estándares de la seguridad informática, ya que este procedimiento debe ser realizado y repetido de manera regular para asegurar la eficacia continua del SGSI.

En todo caso, los controles se detallan siguiendo las orientaciones de ISO 27001:2005 o se pueden elegir de otros conjuntos de control, o incluso diseñados

y desarrollados para solucionar las necesidades importantes de la entidad. El estándar ISO 27002:2013 incluye 114 controles, marcando una diferencia notable con los 133 documentados en la edición anterior de 2005. Estos controles están ahora organizados en catorce secciones en lugar de las once secciones originales.

De manera similar, el estándar ISO IEC 27001 establece que el SGSI garantiza que los procedimientos y actividades de seguridad estén debidamente establecidos para adaptarse a posibles cambios en los riesgos de amenazas, impactos y vulnerabilidades comerciales. Esta es una consideración crucial en un ámbito tan dinámico como la seguridad de la información, destacando así una ventaja fundamental del enfoque adaptable basado en el riesgo de los estándares ISO 27000. La norma abarca organizaciones de todos los tipos, tamaños e industrias o mercados. No obstante, no ofrece directrices precisas sobre controles específicos de seguridad de la información, ya que estos difieren según el tipo de organización. Los controles presentados en ISO IEC 27002 representan una especie de catálogo de opciones disponible, otorgando a la organización la libertad de seleccionar aquellos que resulten apropiados. Además, la certificación basada en ISO / IEC 27001: 2005 requiere una lista bastante larga de información documentada obligatoria sobre SGSI: incluyendo su alcance, política de S.I., evaluación de riesgos y procesos de tratamiento, planificación operativa y documentación de control, e incluso políticas para proveedores o leyes relevantes, regulaciones y obligaciones contractuales más los procedimientos de cumplimiento asociados.

Nuevamente, la edición de 2005 del estándar ISO 27001 se aplicó el modelo PDCA para organizar los controles orientaciones del OECG. En la versión de 27001:2013 enfatiza la evaluación y la medición en el rendimiento óptimo del SGSI de una entidad. También se incluyó una sección sobre contratación externa con esta actualización, prestando mucha observación organizacional en la seguridad informática.

Al mismo tiempo, ISO 27002 es un documento amplio que cubre una amplia gama de riesgos y controles de S.I. que como se ha observado ha crecido a lo largo de todos estos años, convirtiendo la última versión de 2013 en un contenido bastante masivo, debido a tantos cambios relacionados con las tecnologías

cambiantes y los problemas de seguridad informática. Además, carece de referencias tecnológicas actuales de última generación de computación en la nube y BYOD, y también es inconsistente en términos del nivel de descripciones y preocupaciones abordadas. Entonces, el documento ya no se pueda mantener, por lo tanto, es difícil predecir qué pasaría con la estandarización de este artículo en particular.

El estándar ISO 27001 se describe como un manual que establece un conjunto de orientaciones y tiene como objetivo final definir las características para cumplir un objetivo o producto para ser compatible a nivel internacional.

Las normas ISO se describen como el conjunto de normativas que regulan la administración de una empresa en sus diversas áreas. Estas normas ISO fueron establecidas en 1987, como respuesta a la globalización de los mercados, con el objetivo de fortalecer y satisfacer la necesidad de mejorar la competitividad de productos y servicios.

El estándar ISO IEC 27001 fue desarrollada por la CTN entre abril y junio de 2014, tomando el estándar ISO 27001:2013 como referencia.

Las Normas Técnicas Peruanas, según la descripción dada por el Instituto Nacional de Calidad (INACAL) en 2016, se definen como documentos que establecen los requisitos de calidad con el propósito de estandarizar productos, procesos y servicios.

La ISO, que corresponde a las iniciales de International Standardization Organization, es la organización internacional responsable de establecer normas a nivel mundial.

La IEC indica ser **l**a Comisión Electrotécnica Internacional patrocinan la el uso de esta tecnología basado en estas normas o estándares IEC a nivel internacional entre los países en desarrollo.

Del mismo modo, un SGSI engloba políticas, procedimientos, directrices, recursos asociados y actividades que son gestionadas de manera conjunta por una entidad con el objetivo de resguardar su información. Este sistema sigue un modelo sistemático que abarca el establecimiento, ejecución, funcionamiento, supervisión, evaluación, mantenimiento y perfeccionamiento en la seguridad informática de la

entidad para lograr sus planes comerciales. Se apoya en la prueba del riesgo y en los niveles de aceptación del riesgo diseñados por la organización para tratar y encargarse de manera efectiva los riesgos. Por consiguiente, evaluar los requisitos para la protección informática y aplicar los indicadores adecuados para asegurar su resguardo, según sea la necesidad, ocasionando al éxito en la instalación de un SGSI (ISO IEC 27000: 2016 - 3.2.1).

Se puede señalar, el paradigma actual en la seguridad informática, que el ciberataque es un desastre en las organizaciones, posiblemente lo expone a responsabilidades de la OTI, todo esto causa una interrupción en las labores y puede dar lugar a costosas investigaciones técnicas y de reparación.

Además, es importante que sus aplicaciones y flujos de trabajo no sean propensos a errores humanos y que la información no se distorsione a medida que avanza para su organización.

Sin embargo, también hay un impacto a largo plazo debajo de la superficie, las primas de su seguro pueden aumentar y cualquier relación bien establecida con los usuarios se dañará, lo que podría reducir sus ingresos. Peor aún, si una historia llega a los medios locales sobre el ataque, permanecerá en Internet junto con su marca cada vez que un prospecto realice una búsqueda. (Deloitte, 2016)

Por tanto, asegurarse que la reputación esté protegida contra un ataque cibernético o físico de su negocio y la información es de prioridad, aplicarla ayudará a evitar estos riesgos y también se aplicará a sus registros en papel.

La seguridad informática incluye 3 pilares principales: La confidencialidad, la disponibilidad y la integridad para la seguridad informática en la entidad.

La confidencialidad se refiere a la accesibilidad de la información sea únicamente para aquellos autorizados y prohibida a individuos, instituciones o procesos sin autorización, según la definición en la norma ISO IEC 27000:2016 (2.61).

De modo idéntico, la confidencialidad se trata de privacidad y de garantizar que la información solo sea accesible para aquellos con una necesidad probada de verla. La información se puede clasificar como información personal que identifica al paciente y datos confidenciales, como información financiera o de salud.

Finalmente, hay información sensible, como salud sexual o mental, que causaría un daño significativo al paciente si estuviera expuesto. Los pasos para garantizar la confidencialidad deben incluir:

De nuevo, establecer controles o indicadores apropiados para tener acceso a la información y asegurar que el personal acceda apropiadamente a esa información. Una buena práctica es habilitar contraseñas de inicio de sesión y protectores de pantalla con contraseña en su equipo y asegurarse de que los archivos estén guardados.

Al mismo tiempo, se debe asegurar que las computadoras portátiles, tabletas, teléfonos móviles y copias de seguridad estén cifrados, lo que impide el acceso si el dispositivo es robado. Estos dispositivos pueden hacerlo de forma transparente.

Así mismo, es importante asegurarse de que el personal no transmita contraseñas o información confidencial a través de medios no encriptados, y que lleven a cabo las verificaciones apropiadas para verificar la identidad del destinatario. Por lo que, es importante que siempre esté atento a los ataques de ingeniería social, donde los trucos de confianza se utilizan para alentar a los usuarios a entregar información confidencial, o hacer clic en los enlaces que ponen en peligro su equipo.

La integridad se define como la característica de preservar la información y la integridad de sus activos, según lo establecido en la norma ISO 27000:2016 (2.40).

Se puede señalar, que la integridad consiste en garantizar que la información que posee sea precisa, coherente y no se modifique de manera inapropiada. Es importante que sus aplicaciones y flujos de trabajo no sean propensos a errores humanos y que la información no se distorsione a medida que se mueve a través de su organización. Por lo que, siempre se solicita atención a los ataques de ingeniería social, donde se utilizan trucos de confianza para alentar a los usuarios a entregar información confidencial

Los pasos para garantizar la integridad incluyen:

En definitiva, asegurando que su aplicación esté realizando una validación básica de entrada de datos a través de listas desplegables y verificaciones internas de consistencia. Por ejemplo, no esperaríamos que un hombre tenga una bandera de embarazo anterior, o un menor que solicite rellenos dérmicos. En casos como estos, la aplicación debería emitir una alerta y pedir al usuario que verifique nuevamente

Inclusive, si mueve información entre sistemas, realiza auditorías y prueba de 'casos extremos' utilizando datos con valores faltantes y/o extremos para verificar que no se modifiquen.

La disponibilidad implica garantizar que la información y los activos relacionados estén disponibles cuando sean necesarios para los usuarios autorizados, según la definición proporcionada en la norma ISO/IEC 27000:2016 (2.9).

Asimismo, la disponibilidad se centra en asegurar que la información se suministre en el momento que se requiera. Esto significa que su personal debe poder acceder a la información fácilmente para respaldar sus deberes profesionales y que ha tomado las precauciones adecuadas para garantizar que su flujo de trabajo no se vea afectado.

Finalmente, se busca asegurar que su información se respalde regularmente, y que sepa cómo restaurarla, asegurándose de aplicar actualizaciones frecuentes de sistema operativo, aplicaciones y antivirus, asegurándose de tener un plan de contingencia ante los desastres para mantener su negocio en buen estado. Si sus computadoras portátiles fueron robadas o incapacitadas, ¿cómo mantendría funcionando su negocio?

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

De acuerdo con Hernández (1991, p. 5), el análisis se llevó a cabo empleando enfoques cuantitativos, lo que implica la utilización de mediciones numéricas. Esto se traduce en la recopilación de datos con el propósito de examinar hipótesis, apoyándose en análisis estadísticos para identificar patrones de comportamiento.

Este trabajo de investigación se categoriza como investigación aplicada, siguiendo la definición de Murillo (2008). La investigación aplicada, también reconocida como investigación práctica o experimental, se caracteriza por la intención de aplicar los conocimientos existentes mientras se generan nuevos. Esta modalidad implica la implementación y sistematización basadas en la práctica. El propósito de utilizar los resultados y los conocimientos de la investigación es lograr una comprensión coherente, organizada y sistemática de la realidad.

Conforme al autor, la investigación en su diseño adoptado es experimental, y de acuerdo a Santa y Filiberto (2010), hace alusión a la manipulación de una variable experimental no estudiada en condiciones estrictamente controladas, con la finalidad de describir las razones o motivos que generan su ocurrencia.

De acuerdo con la información proporcionada por Ávila (2006, p. 69), se llevó a cabo un estudio pre experimental, caracterizado por la evaluación de una única variable sin ningún control que permitiera la comparación entre grupos. Este diseño se fundamenta en el análisis causal a través de métodos pretest y postest, ya que posibilita la medición antes y después de la implementación de los resultados.

Su representación gráfica es la siguiente:

Figura 1

Diseño preexperimental

3.2 Variables y operacionalización

En un principio se tiene a la variable independiente, NTP ISO IEC 27001, norma o estándar de seguridad informática para las empresas privadas o públicas en la cual se establece un sistema, se implementa y opera, con el fin de mantener y monitorizar, disminuyendo riesgos y amenazas constantes en la información de cada empresa; todo esto para prevenir cualquier eventualidad que atañe la confidencialidad de la información.

En un segundo plano, se encuentra la variable dependiente, que corresponde a la seguridad informática. Esta disciplina engloba varias normas, aplicaciones y mecanismos destinados a salvaguardar la privacidad y la integridad informática en un sistema, así como la de sus usuarios.

Otra interpretación proporcionada por la operacionalización, que se refiere a la aplicación y administración de medidas de seguridad, consta de tres dimensiones fundamentales: confidencialidad, integridad y disponibilidad. Esto implica una diversidad de alertas diseñadas para mitigar los impactos de amenazas que representan riesgos para la seguridad informática. Además, se consigue a través de la utilización de un conjunto de indicadores que engloban aspectos como el control de accesos, la seguridad operativa y la gestión de incidencia en la seguridad informática

3.3 Población, muestra

El escritor Hernández (2014) caracteriza la población como el grupo de casos que satisface ciertos criterios específicos en una entidad, mientras que la muestra se refiere a un subgrupo de esa población (p. 174). En relación con la elección de la población, es relevante indicar que el estudio, que implica a la población, requeriría la participación de 45 personas que trabajan en el área de OGT.

Tabla 1

Distribución de la Población

Área - Cargo	Cantidad de Personas
Gerente de TI	1
Jefe de Desarrollo	1
Sistemas	39
Soporte	4
Total	**45**

Fuente: Elaboración Propia

Población: serán 45 empleados del área de la OGT.

Muestra**.**

No se utiliza una muestra debido al reducido tamaño de la población.

3.4 Técnicas e instrumentos de recolección de datos

Técnica: observación

Se utilizaron métodos de recopilación de datos, como encuestas y cuestionarios, como una herramienta efectiva para diagnosticar la situación presente de la seguridad informática en la OGT de SUCAMEC.

Instrumento de recolección de datos: Ficha de observación.

El instrumento, debidamente segmentado, comprende preguntas derivadas de los indicadores obtenidos de la variable dependiente para su formulación. Con el fin de recabar información requerida, se desarrolló un cuestionario de preguntas con base en los objetivos previamente determinados y distribuidas a toda la muestra para resolver un conjunto de interrogantes estructuradas con opciones de respuesta cerradas.

El cuestionario consta de 25 preguntas o ítems, que pueden considerarse en un anexo, con varias opciones de respuesta para diagnosticar el estado de seguridad de la información.

Conforme a lo indicado por Hernández (2014), la confiabilidad se describe como "el grado en que una herramienta genera productos coherentes y consistentes" (p. 200).

La evaluación de la confiabilidad de la herramienta se realizó mediante la aplicación del coeficiente Alfa de Cronbach. en escalas que contienen varias alternativas de valores. Según Hernández et al. (2012), se definió una escala para evaluar la confiabilidad, tomando como referencia los datos a continuación: Nulo (-1 a 0), confianza muy baja (0, a 0,2), confianza baja (0,2 a 0,4) confiabilidad regular (0,4 a 0,6), confiabilidad aceptable (0,6 a 0,8), confiabilidad alta (0,8 a 1). Asimismo, se empleó el software estadístico IBM SPSS versión 23.0 para analizar los datos experimentales.

A continuación, el grado de confiabilidad del instrumento por cada indicador:

Tabla 2

Confiabilidad del instrumento de seguridad informática.

Dimensión	**Indicador**	**Alfa de Cronbach**
Confidencialidad:	Control de accesos	α: ,967
Integridad de datos:	Seguridad en la operatividad.	α: ,510
Disponibilidad de servicios:	Gestión de incidentes	α: ,654

Fuente: Elaboración Propia

Por lo tanto, cada pregunta o sección está vinculada a la cobertura de dimensiones relacionadas con los indicadores de cada dimensión de la información con base en el estándar ISO 27001 para SUCAMEC OGT.

3.5 Procedimientos

Conforme a la afirmación de Hernández (2014), la validez se relaciona con la medida en que un instrumento efectivamente evalúa una variable (p. 200).

Con el fin de validar el instrumento, se utilizarán enfoques de evaluación a través de un formulario especializado, involucrando la participación de expertos. Este proceso se ejecutará con la intención de perfeccionar los elementos y suprimir cualquier ambigüedad en la redacción, con el objetivo de mejorar la coherencia del instrumento.

Tabla 3

Resultados de validación de la herramienta mediante revisión de expertos.

Instrumento	Expertos			
	Mgtr. Wiliam Romero	Dr. William Flores Sotelo	Mgtr. Joel Visurraga Agüero	Mgtr. Samuel Rivera Castilla
Cuestionario sobre seguridad informática	Aplicable	Aplicable	Aplicable	Aplicable

Fuente: Elaboración Propia

3.6 Método de análisis de datos

Luego que se han obtenido los resultados mediante el uso de la herramienta, se estructuran para su análisis a través de métodos estadísticos descriptivos. Estos resultados se presentarán mediante tablas estadísticas y gráficos, acompañados de su respectivo análisis.

3.7 Aspectos éticos

Para los participantes, se protegieron las identidades del personal de la OGT entrevistados. La información obtenida no será divulgada para ningún otro propósito que no sea la investigación, señalar que, la autorización fue aprobada con consentimiento de la OGT para la realización del estudio. También se cuenta con la colaboración voluntaria de los responsables del departamento de sistemas de la OGT, quienes son especialistas y tienen un entendimiento exhaustivo de todos los procesos en ejecución en la OGT. Finalmente, se asegura la confidencialidad del participante desde el comienzo del estudio.

IV. RESULTADOS

4.1 Análisis de datos

Durante el desarrollo del estudio se describieron los resultados de los análisis descriptivos e inferenciales.

En el análisis descriptivo se utilizó el estándar ISO 27001 para evaluar el impacto significativo de los 3 pilares en la seguridad informática en OGT SUCAMEC; Se aplicó el pretest para recolectar información sobre el estado inicial de los tres índices; luego aplicar estándar ISO/IEC 27001 y reevaluar el estado post-test de los indicadores en SUCAMEC OGT.

Confidencialidad

Tabla 4

Análisis de fiabilidad del Pretest y Postest de control de accesos

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,967	45

Fuente: Elaboración propia asistida por IBM SPSS versión 23

Después de examinar los resultados obtenidos a través del software SPSS, se evidencia un coeficiente Alfa de Cronbach de ,967, indicando un alto grado de confiabilidad.

Tabla 5

Medidas descriptivas del Pretest y Postest de control de accesos

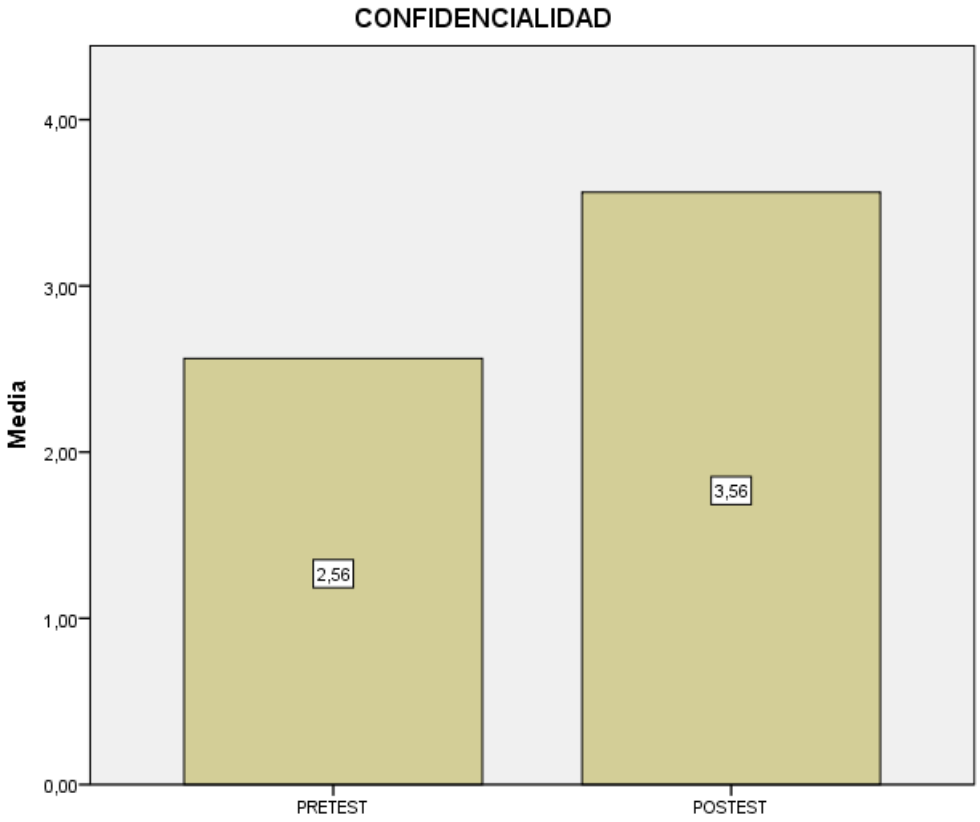
Estadísticos descriptivos					
	N	Mínimo	Máximo	Media	Desviación estándar
PRETEST	45	2,18	2,87	2,5633	,24274
POSTEST	45	3,27	3,82	3,5633	,19144
N válido (por lista)	45				

Fuente: Elaboración propia asistida por IBM SPSS versión 23

En este orden, los resultados obtenidos con el software SPSS arrojan un promedio de 2.5633 para el pretest, mientras que en el postest logramos un promedio de 3.5633, lo que nos permite observar mejoras en el indicador de control de acceso, con un aumento de 1.0

Figura 2

Gráfico de barras del Pretest y Post Test de control en accesos

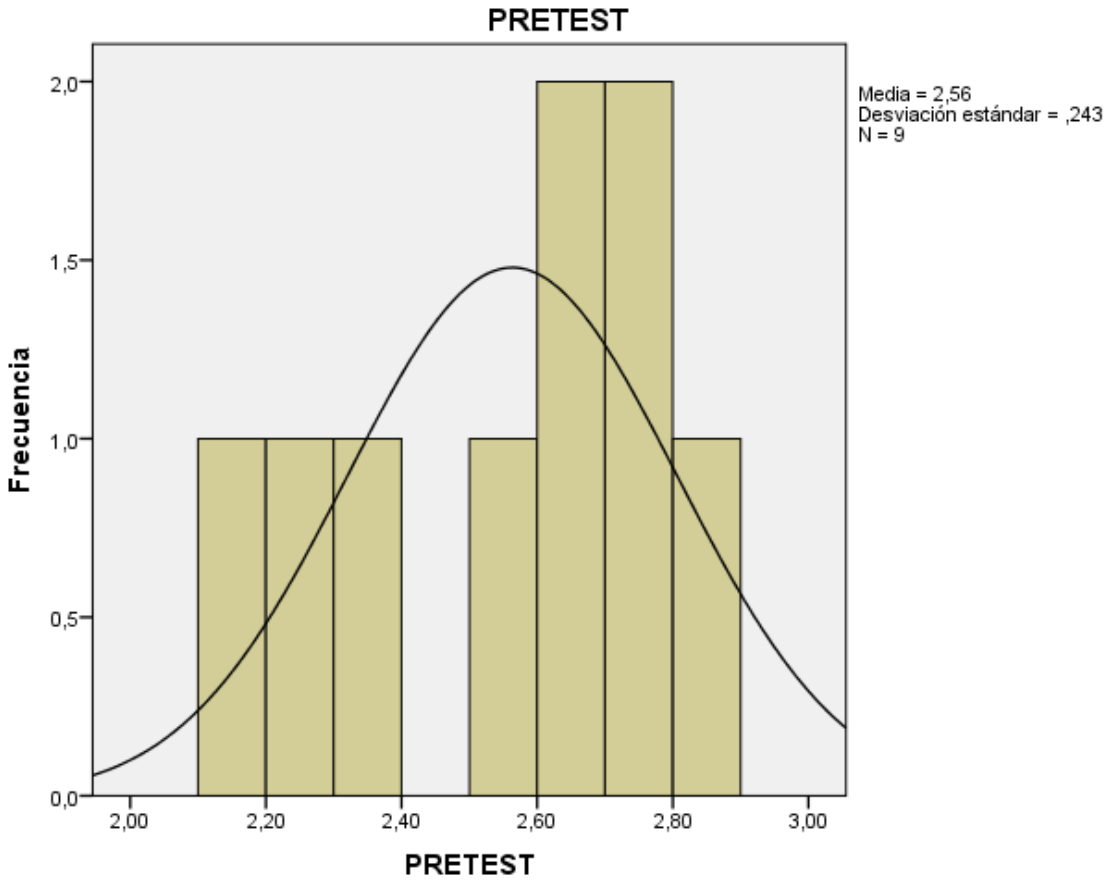


Fuente: Elaboración propia asistida por IBM SPSS versión 23

En el gráfico de barras se puede observar la información de la prueba anterior con un nivel de 2,56 para el indicador de control de acceso, mientras que luego de aplicar la norma NTP ISO 27001 se logró una mejora, logrando el Punto 3,56 referente al control de acceso.

Figura 3

Gráfico de histograma del Pretest de control de accesos

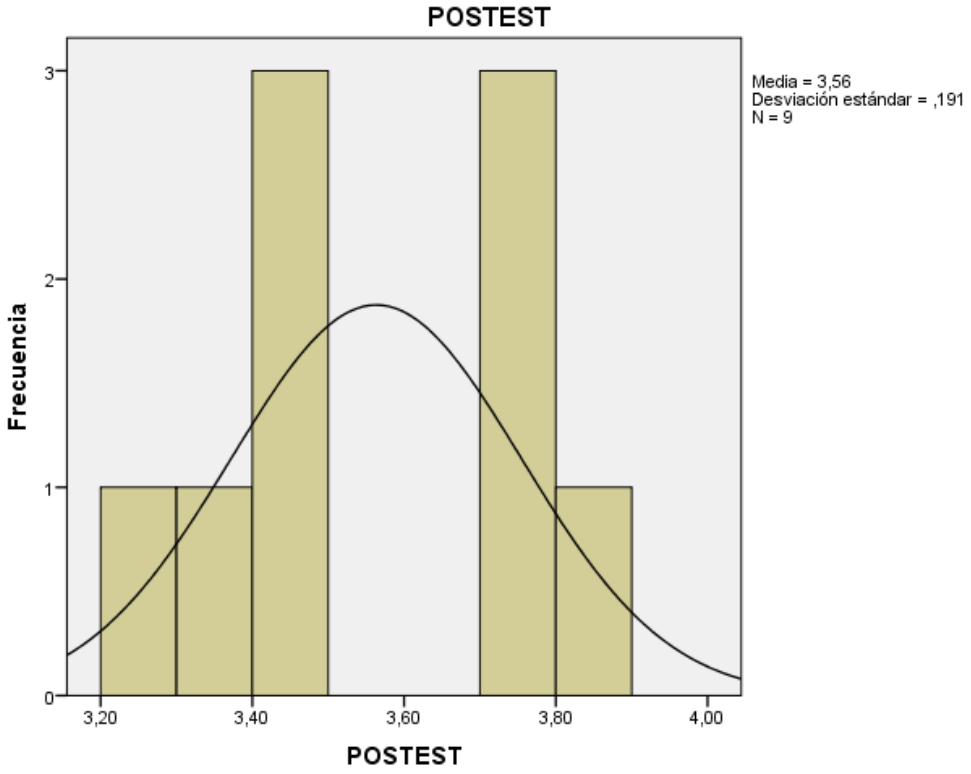


Fuente: Elaboración propia asistida por IBM SPSS versión 23

Para la gráfica con la curva se puede observar que el resultado de la media durante el pretest fue de 2,56 con una desviación estándar de ,243.

Figura 4

Gráfico de histograma del Post Test de control de accesos



Fuente: Elaboración propia asistida por IBM SPSS versión 23

Para la gráfica con la curva se puede observar que el resultado de la media durante el postest es 3,56 con una desviación estándar de ,191

Análisis Inferencial

En la evaluación subsiguiente, se emplea el test de normalidad utilizando el método de Shapiro-Wilk para nuestros tres indicadores.

Es relevante destacar que la confirmación de la normalidad se regirá por ciertos criterios, los cuales se examinarán con base en la información recopilada durante el procesamiento de los datos.

Cuando el nivel de significancia es menor a 0,05, se trata de una distribución no normal.

Cuando el nivel de significancia es mayor a 0,05, se trata de una distribución normal.

Tabla 6

Test de normalidad del Pretest y Postest de control de accesos.

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRETEST	,161	45	,200*	,933	45	,511
POSTEST	,223	45	,200*	,927	45	,456

*. Esto es un límite inferior de la significación verdadera.

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia asistida por IBM SPSS versión 23

Se puede apreciar que el nivel en la significancia es de ,511 para el pretest y ,456 para el postest, valores superiores a 0,05. Por ende, se infiere que se tiene una distribución normal, lo que viabiliza la aplicación de estadísticas paramétricas. Con este fin, se ejecuta la prueba para calcular la distribución T-Student, obteniendo los siguientes datos:

Tabla 7

Prueba T del Pretest y Postest de control de accesos

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desviación estándar	Media de error estándar	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	POSTEST - PRETEST	1,00000	,07858	,02619	,93960	1,06040	38,177	45	,000

Fuente: Elaboración propia asistida por IBM SPSS versión 23

El valor en la significancia obtenido de la prueba t es 0,000, el cual es inferior a 0,05. Por consiguiente, se descarta la hipótesis nula y se toma la hipótesis alternativa.

Integridad

Tabla 8

Análisis de fiabilidad del Pretest y Postest en seguridad para la operatividad

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,510	45

Fuente: Elaboración propia asistida por IBM SPSS versión 23

En la tabla, corroboramos que los datos obtenidos a través del programa SPSS revelan un coeficiente Alfa de Cronbach de ,510, indicando un alto grado de confiabilidad.

Tabla 9

Medidas descriptivas del Pretest y Postest de seguridad de la operatividad

Estadísticos descriptivos

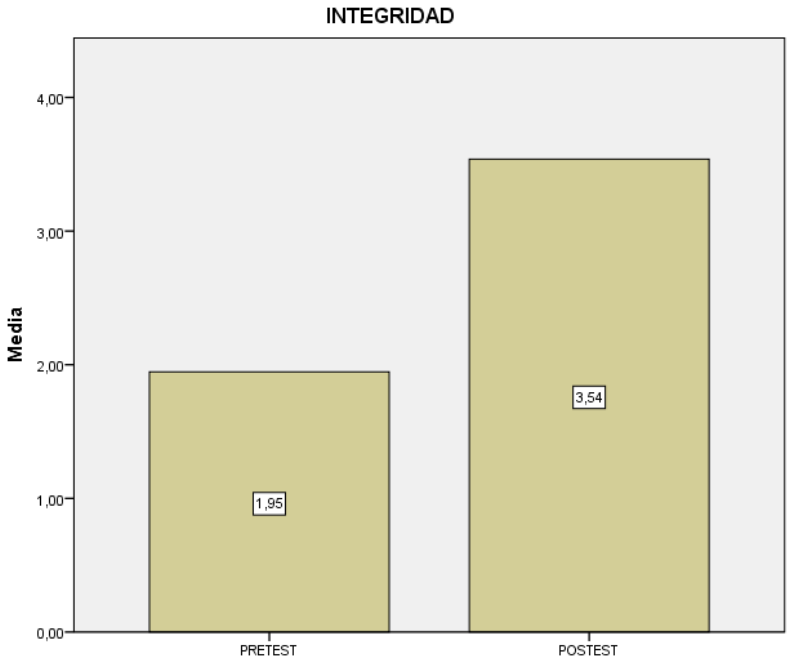
	N	Mínimo	Máximo	Media	Desviación estándar
PRETEST	45	1,67	2,02	1,9463	,12682
POSTEST	45	3,47	3,82	3,5388	,13346
N válido (por lista)	45				

Fuente: Elaboración propia asistida por IBM SPSS versión 23

Según información de la tabla, verificamos que los resultados derivados del programa SPSS revelaron una media de 1,9463 para el pretest, mientras que para el postest la media fue de 3,5388, indicando una mejora en la seguridad operacional con un incremento de 1,59.

Figura 5

Gráfico de barras del Pretest y Postest de seguridad de la operatividad

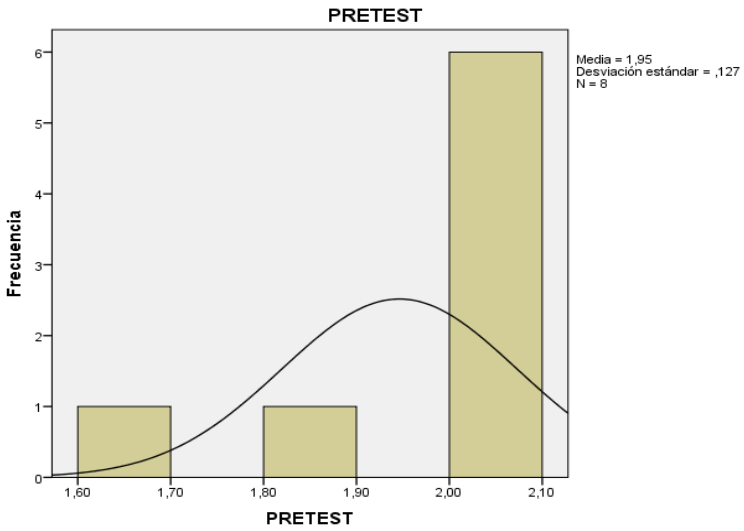


Fuente: Elaboración propia asistida por IBM SPSS versión 23

En el gráfico de barras se puede observar información de la prueba anterior con 1,95 en cuanto a seguridad operacional, mientras que luego de aplicar la norma NTP ISO 27001 se logró una mejora logrando un resultado de 3,54 en seguridad operacional.

Figura 6

Gráfico de histograma del Pretest de seguridad de la operatividad

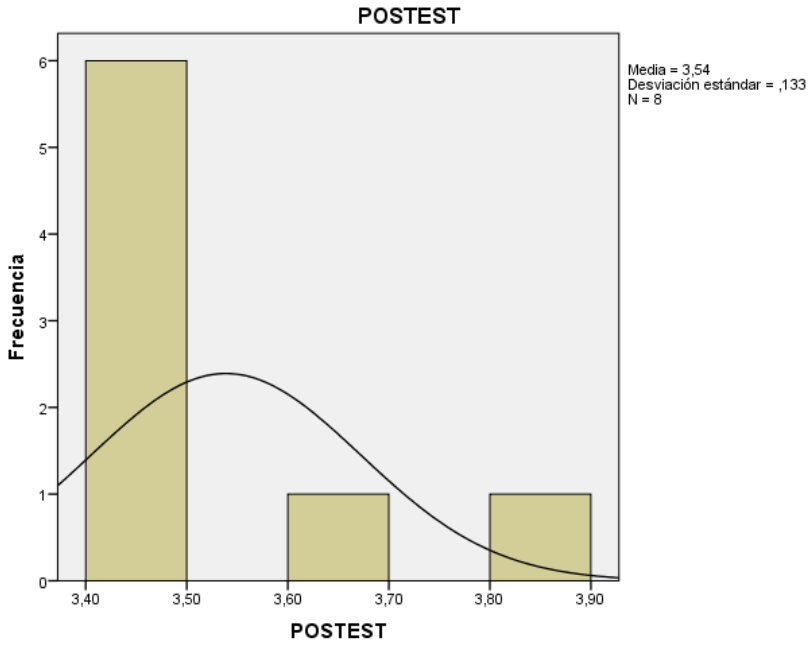


Fuente: Elaboración propia asistida por IBM SPSS versión 23

La representación gráfica con la curva permite visualizar que el valor medio durante el pretest fue de 1,95, con una desviación estándar de ,127.

Figura 7

Gráfico de histograma del Post Test de seguridad de la operatividad



Fuente: Elaboración propia asistida por IBM SPSS versión 23

La representación gráfica con la curva se puede observar que el resultado de la media durante el postest es 3,54 con una desviación estándar de 0,133.

Análisis Inferencial

En la evaluación subsiguiente, se utiliza la prueba de normalidad para nuestros tres indicadores, debiendo aplicarse un test basado en el método Shapiro-Wilk.

Es importante destacar que la evaluación del pretest sigue ciertos parámetros, los cuales serán analizados tomando como base a la información recabada durante el procesamiento de datos.

Cuando el nivel de significancia es menor a 0,05, indica que se trata de una distribución no normal.

Cuando el nivel de significancia es mayor a 0,05, indica que se trata de una distribución normal.

Tabla 10

Prueba de normalidad del Pretest y Postest de seguridad de la operatividad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRETEST	,414	45	,000	,658	45	,011
POSTEST	,447	45	,000	,607	45	,016

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia asistida por IBM SPSS versión 23

En la tabla previa se evidencia que el nivel de significancia es ,011 para el pretest y ,016 para el postest, cifras superiores a 0,05. Por ende, se concluye que se presenta una distribución normal, permitiendo así el empleo de estadísticas paramétricas.

Con este propósito, se realiza la prueba para calcular la distribución T-Student, obteniendo los siguientes resultados:

Tabla 11

Prueba T del Pretest y Postest de seguridad de la operatividad

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desviación estándar	Media de error estándar	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	POSTEST - PRETEST	1,59250	,14936	,05281	1,46764	1,71736	30,158	45	,000

Fuente: Elaboración propia asistida por IBM SPSS versión 23

La significancia encontrada en la prueba t es 0,000, que es menor que 0,05, por lo que se rechaza la hipótesis nula y se acepta la hipótesis alternativa.

Disponibilidad

Tabla 12

Análisis de fiabilidad del Pretest y Postest de gestión de incidentes

Estadísticas de fiabilidad

Alfa de Cronbach	N de elementos
,654	45

Fuente: Elaboración propia asistida por IBM SPSS versión 23

Tras analizar los resultados derivados del programa SPSS, se presenta un coeficiente Alfa de Cronbach de ,654, indicando un elevado grado de confiabilidad.

Tabla 13

Medidas descriptivas del Pretest y Postest de gestión de incidentes

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
PRETEST	45	1,76	2,42	2,0038	,25360
POSTEST	45	3,64	3,82	3,7100	,07131
N válido (por lista)	45				

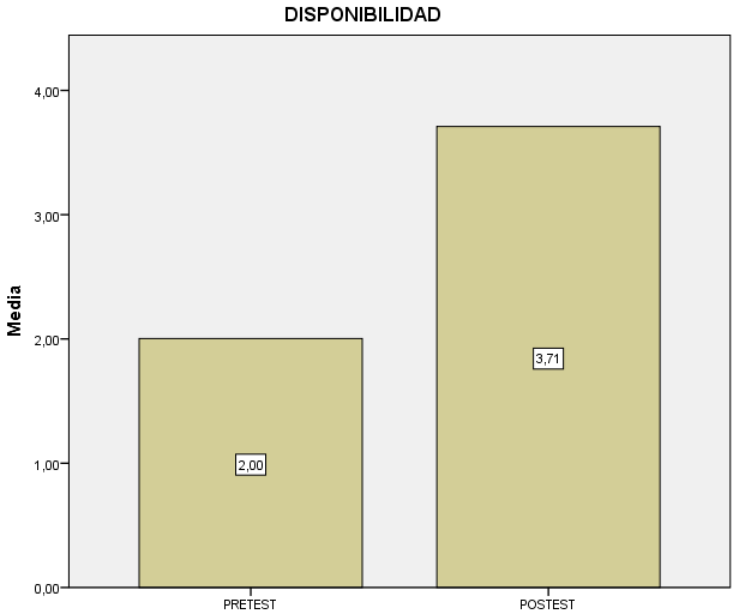
Fuente: Elaboración propia asistida por IBM SPSS versión 23

Tras analizar los resultados obtenidos a través del programa SPSS, se observó que el promedio del pretest fue de 2,5633, mientras que el del postest fue

de 3,5633, señalando una mejora en los indicadores de gestión de incidentes de seguridad de la información, con un aumento de 1,70.

Figura 8

Gráfico de barras del Pretest y Postest de gestión de incidentes.

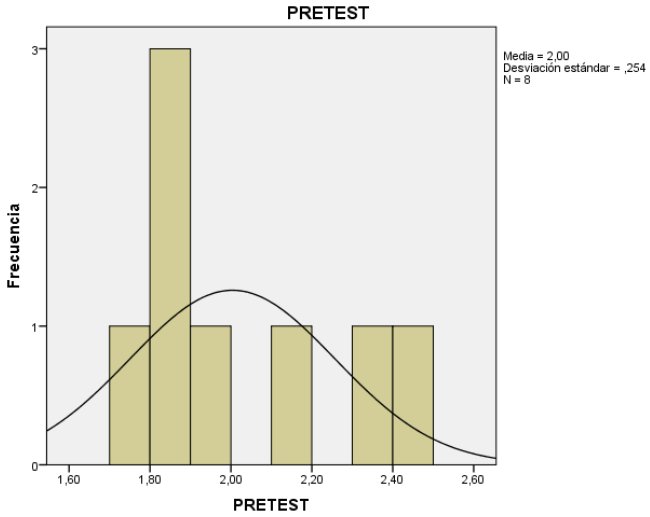


Fuente: Elaboración propia asistida por IBM SPSS versión 23

En el gráfico de barras se puede observar información de la prueba anterior con un puntaje de 2,00 en Gestión de Incidentes de Seguridad Informática, mientras que luego de aplicar la Norma ISO 27001 se logró una mejora con un puntaje de 3,71, en Gestión de Incidentes de Seguridad Informática

Figura 9

Gráfico de histograma Pretest en gestión de incidentes

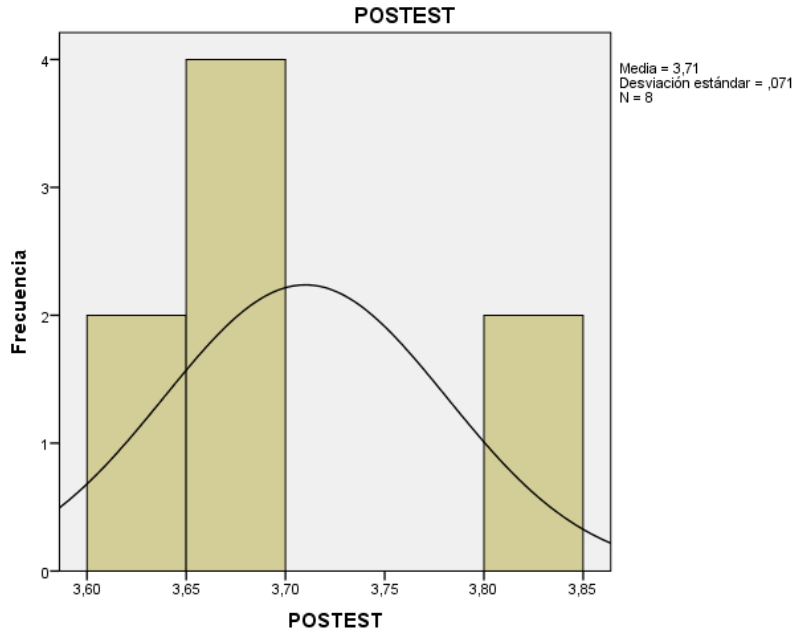


Fuente: Elaboración propia asistida por IBM SPSS versión 23

En la gráfica con la curva se puede observar que el resultado de la media durante el pretest fue 2,00 con una desviación estándar de ,254.

Figura 10

Gráfico de histograma Post Test en gestión de incidentes



Fuente: Elaboración propia asistida por IBM SPSS versión 23

En la gráfica con la curva se puede ver que el resultado de la media en el siguiente postest es 3,71 con una desviación estándar de ,071.

Análisis Inferencial

En el siguiente análisis, se ejecuta la prueba de normalidad para los tres indicadores, utilizando un método basado en la normalidad de Shapiro-Wilk.

Es relevante destacar que la prueba inicial se guía por determinados criterios, los cuales se analizarán considerando los datos recabados durante su procesamiento.

Cuando la significancia del nivel es menor a 0,05, se trata de una distribución no normal.

Cuando la significancia del nivel es mayor a 0,05, se trata de una distribución normal.

Tabla 14

Prueba de normalidad Pretest y Postest en gestión de incidentes

Pruebas de normalidad

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
PRETEST	,241	45	,192	,844	45	,083
POSTEST	,360	45	,003	,773	45	,014

a. Corrección de significación de Lilliefors

Fuente: Elaboración propia asistida por IBM SPSS versión 23

Se observa que la significancia del nivel es de ,83 para el pretest y ,014 para el postest, valores superiores a 0,05. En consecuencia, se determina que hay una distribución normal, posibilitando el uso de estadísticas paramétricas.

Con este propósito, se lleva a cabo la prueba de cálculo de la distribución T-Student, obteniendo los datos presentados a continuación:

Tabla 15

Prueba T Pre Test y Post Test en gestión de incidentes

Prueba de muestras emparejadas

		Diferencias emparejadas							
					95% de intervalo de confianza de la diferencia				
		Media	Desviación estándar	Media de error estándar	Inferior	Superior	t	gl	Sig. (bilateral)
Par 1	POSTEST - PRETEST	1,70625	,18898	,06681	1,54826	1,86424	25,537	45	,000

Fuente: Elaboración propia asistida por IBM SPSS versión 23

El nivel de significancia obtenido en la prueba T es 0.000, lo cual es inferior a 0.05. En consecuencia, descartamos la hipótesis nula y tomamos la hipótesis alternativa.

V. DISCUSIÓN

En el marco de esta investigación, se examinaron los resultados derivados de este estudio, comparando los indicadores de control de acceso, seguridad operativa y gestión de incidentes en las pruebas previas y posteriores a la implementación del estándar ISO 27001 en la seguridad informática de la OGT SUCAMEC.

Por lo tanto, en la medición previa, el índice de control de acceso promedió 2.56, y después de implementar la Normativa ISO 27001, se incrementó a 3.56. Los datos indican que con la instalación de la NTP, el aumento al 1.0 representa el 39.1%, afectando de manera significativa el control de accesos en la OGT de SUCAMEC.

De manera significativa, el estudio llevado a cabo por Barrantes, C (2012), evidenció que la concepción e instauración de un SGSI resulta un incremento del 72% al 78.5% en términos de seguridad. Esto se consigue mediante la aplicación de políticas de seguridad vinculadas a los activos informáticos de la empresa Card Perú, garantizando que los riesgos de seguridad informática se identifiquen, asuman, administren y mitiguen.

Asimismo, en las mediciones iniciales, el índice de seguridad operacional tuvo un promedio de 1.95 y, tras la implementación de la norma NTP ISO 27001, se incrementó a 3.94. Los resultados señalan que la implementación de la NTP tiene un impacto considerable de 1.99, representando el 102.1%, en la seguridad operacional en la OGT de SUCAMEC.

A partir de esta investigación llevada a cabo por Alcántara, J. (2015), se concluye que la aplicación de la seguridad basada en el estándar ISO 27001 ha mejorado la seguridad informática en las operaciones, incrementando los niveles de seguridad a un 44% en relación con la prevención de riesgos de seguridad informática.

Por ende, el índice en gestión para los incidentes en la seguridad informática en su medición previa promedió 2.0, y al implementar la norma NTP ISO 27001, este índice aumentó a 3.71. Los resultados señalan que la implementación de la NTP, con un incremento de 1.71, que representa el 85.5%, tiene un impacto

sustancial en la gestión de incidentes del ámbito de la seguridad informática en la OGT SUCAMEC.

En síntesis, según un estudio realizada por Alcántara, J. (2015), se evidenció que la aplicación de la seguridad basada en el estándar ISO 27001 mejoró las capacidades de seguridad para encontrar anomalías y fallas en la seguridad informática, incrementando los niveles en 44% para prevenir riesgos asociados con la seguridad informática.

VI. CONCLUSIONES

Primero:

Con base en los resultados alcanzados, se deduce que la seguridad informática en la OGT ha experimentado una mejora significativa gracias a la adopción del estándar ISO 27001.

Segundo:

El indicador control de acceso nos permite evaluar la información de la prueba anterior con 2.56, mientras que luego de aplicar la Norma ISO 27001 se obtiene un resultado de 3.56, lo que representa un 39,1% en Norma ISO 27001 aplicada y que afecta significativamente la seguridad informática de la OGT SUCAMEC.

Tercero:

El índice de seguridad operacional nos brinda la oportunidad de evaluar la información antes de realizar la prueba con una puntuación de 1.95, mientras que después de aplicar la normativa ISO 27001, el resultado es de 3.94, representando un incremento del 102.1%. En relación con la aplicación de la normativa ISO 27001, impacta de manera significativa la Seguridad Informática en su integridad de la OGT SUCAMEC.

Cuarto:

El indicador de gestión de incidentes de la seguridad informática nos permitió evaluar la información del pretest con 2.0 mientras que luego de aplicar la NTP ISO/IEC 27001 obtuvo un resultado de 3.71, esto representa un 85.5% que la normativa ISO 27001 afecta significativamente la disponibilidad de la seguridad de la informática de la OGT SUCAMEC.

Finalmente se puede concluir que el estándar ISO 27001 y su aplicación afecta significativamente la seguridad informática en la OGT SUCAMEC.

VII. RECOMENDACIONES

Primero:

Se recomienda aplicar el estándar ISO 27001 para mejorar el control de accesos, la seguridad operativa y las capacidades de gestión de incidentes de OGT SUCAMEC, para proteger la seguridad informática, proteger los procedimientos de TI, evitar amenazas tanto como prevenir situaciones que dañen la información importante de la Institución SUCAMEC.

Segundo:

Se recomienda que el personal de OGT sean capacitados por expertos en Seguridad Informática en la norma Normativa ISO 27001, así como programar charlas de acuerdo con el valor que hoy se da a los tres pilares de la seguridad informática.

Tercero:

Se sugiere otorgar prioridad a la obtención de la certificación internacional ISO 27001 para el personal calificado en TI, con el propósito de asegurar la seguridad informática para la OGT SUCAMEC.

.

REFERENCIAS

Aguilera. (2008). *Purificación, Seguridad Informática.* Editex.

Alcántara, J.C. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P. en la ciudad de Chiclayo*. [Tesis de ingeniería, Universidad Católica Santo Toribio de Mogrovejo]. http://hdl.handle.net/20.500.12423/539

Andrade C., Chávez C. (2018). *Generación de un plan para la gestión integral de seguridad de la información basado en el marco de la norma ISO 27001 y las mejores prácticas de seguridad de la norma ISO 27002 para la compañía internacional GYM ECUAINTERGYM S.A. de la ciudad de Guayaquil*. [Facultad de ingeniería, Universidad de Guayaquil]. http://repositorio.ug.edu.ec/handle/redug/32606

Amutio, M., & Candau, J. (2012). *MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Ministerio de Hacienda y Administraciones Públicas

Areito, J. (2008). *Seguridad de la Información, Redes, informática y sistemas de información.* Paraninfo.

Barrantes, C., & J. H. (2012*). Diseño e implementación de un Sistema de Gestión de Seguridad de Información en procesos tecnológicos*. Universidad de San Martín de Porres.

Bernal, C. (2010). *Metodología de la investigación, administración economía, humanidades y ciencias sociales*. Pearson.

Bolhari, A. (2009). Electronic-Supply Chain Information Security: A Framework for Information. Australian Information Security Management Conference.

Bowman, R. J. (2013). *Why Cybersecurity Is a Supply-Chain Problem..* Think Tank

Calder A., Watkins S. (2019). *Information Security Risk Management for ISO 27001/ISO 27002*. United Kingdom: IT Governance Publishing Ltd.

Caso de éxito: ISO 27001. (s.f.). aplicada en el Sector Público. Obtenido de https://www.isotools.cl/caso-exito-iso-27001-aplicada-sector-publico/

Ciclo PDCA. (s.f.). (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua | PDCA Home. Obtenido de http://www.pdcahome.com/5202/ciclo-pdca/

Costas, J. (2010). *Seguridad Informática.* RA-MA Editorial.

Gomés, Á., & Suárez, C. (2011). *Sistemas de Información. Herramientas prácticas para la gestión.* (3° ed.). Alfa y Omega Grupo Editor.

Gómez F., y Católico D. (2010). Relación de la presentación de información de negocios on-line con las variables financieras en las empresas colombianas. *Revista Facultad de Ciencias Económicas: Investigación y Reflexión, 18*(1), 205-224. Recuperado de https://bit.ly/2RtJRp3

Guerrero, Z., Tivisay, M., Flores, H., & Hazel, C. (2009). *Teorias do aprendizagem e a instrução no desenho de materiais didáticos informáticos.* Educere.

Guzmán, C. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad Financiera de Segundo Piso*. [Tesis de ingeniería, Institución Universitaria Politécnico Grancolombiano]. http://hdl.handle.net/10823/654

Hernández, R., Fernández, C., & Baptista, P. (2010). *Metodología de la investigación*. (4° ed.). McGraw - HILL/Interamericana editores.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la Investigación*. McGraw - HILL/Interamericana editores.

Information security management. (s.f.). Obtenido de http://www.iso.org/iso/iso27001

Instituto Nacional de Calidad. (s.f.). Normas Técnicas Peruanas (NTP) - INACAL. http://www.inacal.gob.pe/principal/categoria/normas-tecnicas-peruanas

ISACA. (s.f.). Information Systems Audit and Control Association -en español - La integridad de los datos: el aspecto más relegado de la seguridad de la información. http://www.isaca.org/JOURNAL/ARCHIVES/2011/VOLUME-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation- spanish.aspx

ISO 27001. (2013). Information Security Management.

ISO en español. (s.f.). Portal de ISO 27001 en español. Obtenido de http://www.iso27000.es/

ISO/IEC 27000. (2014). Information technology — Security techniques — Information security management systems — Overview and vocabulary.

ISO/IEC 27001. (s.f.). Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27001. (s.f.). ISO Management system standards.

ISO/IEC 27002. (2013). Information technology — Security techniques — Code of practice for information security controls.

ISO/IEC 27003. (2010). Information technology — Security techniques — Information security management system implementation guidance.

ISO/IEC 27004. (2009). Information technology — Security techniques — Information security management — Measurement.

ISO/IEC 27005. (2011). Information technology — Security techniques — Information security risk management.

ISO/IEC 27006. (2011). Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems.

ISO/IEC 27007. (2011). Information technology — Security techniques — Guidelines for information security management systems auditing.

Isotools. (s.f.). ¿Qué son las normas ISO y cuál es su finalidad? Obtenido de https://www.isotools.org/2015/03/19/que-son-las-normas-iso-y-cual-es-su-finalidad/

Lapiedra, R., Devece, C., & Guiral, J. (2011). Introducción a la gestión de sistemas de información en la empresa. Colección Sapientia.

Monteza, L.O. (2020). *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.* [Tesis de ingieneria, Universidad Peruana de Ciencias Aplicadas]. http://hdl.handle.net/10757/652121

Norma Tecnica Peruana (2° ed.). (2014). Lima.

Norma Tecnica Peruana. (2014). Lima.

Ortiz, R.M y Prada, G.A. (2022). *Diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área de Tecnologías de la Información y la Comunicación del Hospital San Vicente de Paúl de Fresno.* [Tesis de posgrado, Universidad Nacional Abierta y a Distancia – UNAD]. https://repository.unad.edu.co/handle/10596/51482

PAe - MAGERIT. (s.f.). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Obtenido de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WZEEgVXyj7A

Peñafiel, C, A. (2019). *Diseño de un modelo para establecer un sistema de gestión de la seguridad de la información dentro de un ambiente Cloud Computing, aplicando la Norma ISO 27001:2013.* [Tesis de posgrado, Universidad Catolica del Ecuador]. http://repositorio.puce.edu.ec:80/handle/22000/17785

PMI. (s.f.). Project Management Institute. Obtenido de http://pmi.org.py/index.php/pmi/

Quezada, N. (2010). Metodología de la investigación, estadística aplicada en la investigación. Perú: Empresa Editorial Macro.

Ramírez, J. P. (2021). *Diseño de un sistema de gestión de seguridad de la información para los procesos de soporte y desarrollo de software en la empresa ALFCOM S.A basado en la norma ISO/IEC 27001:2013*. [Tesis de posgrado, Universidad Piloto de Colombia] http://repository.unipiloto.edu.co/handle/20.500.12277/11101

Revista Bibliográfica de Geografía y Ciencias Sociales. (1998). Las normas ISO. Obtenido de http://www.ub.edu/geocrit/b3w-129.htm

Roy, A., & Kundu, A. (2012). Management of information security in supply chains–a process framework. South Africa.

Santos D. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software. Perú*. [Tesis de ingeniería, universidad católica del Perú]. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7616

Según Normas ISO. (s.f.). Obtenido de http://www.unlu.edu.ar/~ope20156/normasiso.htm

Talavera, V. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud de acuerdo a la ISO/IEC 27001.* [Tesis de ingeniería, Pontificia Universidad Católica del Perú]. http://hdl.handle.net/20.500.12404/6092

Torres, J.P y Asqui, J.A. (2023). *27001 para mejorar la seguridad de la información en una institución educativa, Lima 2022*. [Tesis de Ingeniería, Universidad Norbert Wiener]. https://hdl.handle.net/20.500.13053/8519

Tola, D. (2015). Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de Consultoría y Auditoría aplicando la norma ISO/IEC. Ecuador: Escuela Superior Politécnica del Litoral.

Vilca E. (2017). *Diseño e implementación de un SGSI ISO 27001 para la mejora de la seguridad del área de recursos humanos de la empresa Geosurvey de la ciudad de Lima*. [Universidad de inguinaria, Universidad de Huánuco]. http://repositorio.udh.edu.pe/123456789/809

Villadeza, K.L y Condor, R.D. (2022). *Diseño de un sistema de gestión de seguridad de la información basado en la norma técnica Peruana -ISO/IEC 27001:2014 para la municipalidad distrital de Huácar 2022*. [Tesis de Ingeniería, Universidad Nacional Hermilio Valdizán]. https://repositorio.unheval.edu.pe/bitstream/handle/20.500.13080/8238/TIS00137V66.pdf?sequence=1&isAllowed=y

Web Electrónica

www.iso270012013.info (www.rsm.nl and security-today.com)

www.iso.org

www.iso27001security.com

www.27000.org

ANEXOS

Anexo 1. Cuestionario Seguridad Informática

TÍTULO: Aplicación de la Norma Técnica Peruana ISO - IEC 27001 en la seguridad informática de la Oficina General de Tecnologías de la SUCAMEC

OBJETIVO GENERAL: Determinar en qué medida la aplicación del modelo NTP ISO/IEC 27001 mejora la seguridad informática en la OGTIC de SUCAMEC

INSTRUCCIONES: Marque con una (X) según crea Ud. conveniente su respuesta.

DATOS GENERALES:

Edad ..... Sexo …… Nivel Académico ……. Distrito…….

LEYENDA:

0	1	2	3	4
NUNCA	**CASI NUNCA**	**ALGUNAS VECES**	**CASI SIEMPRE**	**SIEMPRE**

	SEGURIDAD DE LA INFORMACION	0	1	2	3	4
D1	**CONFIDENCIALIDAD DE INFORMACIÓN.**					
1	¿Se realiza una verificación de los antecedentes de los candidatos para ocupar cargos administrativos, contratistas y usuarios externos de acuerdo con las leyes, reglamentaciones y ética pertinentes a los requisitos de la OGT para la clasificación de información a ser ingresado y los riesgos percibidos?					
2	¿La OGT aplica procesos disciplinarios a los usuarios que cometan un incumplimiento de seguridad?					
3	¿Se vigilan la moral y el comportamiento del personal que maneja los sistemas de información con el fin de mantener una buena imagen y evitar un posible fraude?					
4	¿Se dan directrices para clasificar la información de acuerdo con su valor, requisitos legales, sensibilidad y criticidad para la OGT?					
5	¿Se retiran los derechos de acceso a todos los empleados, contratistas y usuarios a la información y al recurso para el procesamiento de la información una vez terminado su empleo, contrato o acuerdo, o una vez realizado el cambio a otra dependencia?					
6	¿La OGT se asegura de que los empleados, contratista y usuarios devuelvan todos los activos de la OGT que posean una vez terminado su empleo, contrato o acuerdo?					
7	¿Se establecen, documentan y revisan las políticas de control de accesos a la información?					
8	¿Se controla a través de un proceso de gestión formal la asignación de contraseñas de usuarios para prevenir el acceso no autorizado a los sistemas de información?					

9	¿Se desarrollan e implementan políticas sobre la utilización de controles para la protección de confidencialidad de la información?					
D2	**INTEGRIDAD DE DATOS**					
10	¿Se realizan mantenimientos preventivos a los equipos a fin de asegurar su continua disponibilidad e integridad?					
11	¿Se toman las previsiones para que todos los dispositivos de almacenamiento de datos (Pendrive, CD, Disco duros, entre otros), sean eliminados o formateado completamente antes de su utilización?					
12	¿La OGT da instrucciones claras y firmes a los usuarios para que prohíban el traslado o retiro de equipo, información o software sin autorización?					
13	¿Se controlan los cambios de los recursos y sistemas de procesamiento de la información?)					
14	¿Se realizan seguimientos, ajustes y proyecciones de los requisitos de la capacidad futura de la utilización de los recursos, para garantizar el desempeño del sistema requerido?					
15	¿Se gestionan y controlan adecuadamente la red de datos a fin de protegerla de las amenazas y mantener la seguridad para los sistemas y aplicaciones que utiliza la red, incluyendo la información en tránsito?					
16	¿Se realizan análisis y especificaciones de seguridad para los nuevos sistemas de información o para las mejoras de los sistemas existentes?					
17	¿Se desarrollan e implementan políticas sobre la utilización de controles para la protección de la integridad de datos?					
D3	**DISPONIBILIDAD DE SERVICIOS.**					
18	¿La OGT toma medidas concretas para evitar el robo de equipos tales como laptops y otros componentes?					
19	¿Se diseñan y aplican protección física a la información contra el daño por fuego, inundación, sismo, explosión, disturbios, y las otras formas de desastre natural o hecho por el hombre?					
20	¿Se protegen los equipos contra fallas de energía y otras interrupciones eléctricas causadas por problemas en los servicios de apoyo?					
21	¿Se protegen debidamente el cableado de energía eléctrica y de comunicaciones que transporta datos contra la interceptación o daños?					
22	¿Se les solicita a todos los usuarios de los sistemas y servicios de información reportar cualquier debilidad en la seguridad de los sistemas o servicios, que haya sido observada o sospechada?					
23	¿Se establecen las responsabilidades y procedimiento de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de información?					
24	¿Se desarrollan e implementan planes para mantener y recuperar las operaciones y asegurar la disponibilidad de la información al					

	nivel requerido y en los plazos requeridos, tras la interrupción o la falla de los procesos críticos de la OGT?					
25	¿Se desarrollan e implementan políticas sobre la utilización de controles para la disponibilidad de servicios?					

Anexo 2. Matriz de consistência

Título: Aplicación de la Norma Técnica Peruana ISO - IEC 27001 en la seguridad informática de la Oficina General de Tecnologías de la SUCAMEC

Autor: DANTE GONZALO SACRAVILCA NARCISO

Problema	Objetivos	Hipótesis	Variables e indicadores				
			Variable : Seguridad de la información				
			Dimensiones	**Indicadores**	**Ítems**	**Escala de medición**	**Niveles o rangos**
Problema General: ¿En qué medida la aplicación de la NTP ISO/IEC 27001 Influye en la seguridad informática de la OGTIC de SUCAMEC? **Problemas específicos.** ¿En qué medida la aplicación de la NTP ISO/IEC 27001 influye en la confidencialidad de la seguridad informática en la OGTIC de SUCAMEC? ¿En qué medida la aplicación de la NTP ISO/IEC 27001 influye en la integridad de la seguridad informática en la OGTIC de SUCAMEC? ¿En qué medida la aplicación del modelo NTP ISO/IEC 27001 influye en la disponibilidad de la seguridad informática en la OGTIC de SUCAMEC?	**Objetivo general:** Determinar en qué medida la aplicación del modelo NTP ISO/IEC 27001 mejora la seguridad informática en la OGTIC de SUCAMEC **Objetivos Específicos** Determinar la influencia de la NTP ISO/IEC 27001 en la confidencialidad de la seguridad informática en la OGTIC de SUCAMEC. Determinar la influencia de la NTP ISO/IEC 27001 en la integridad de la seguridad informática en la OGTIC de SUCAMEC. Determinar la influencia de la NTP ISO/IEC 27001 en la disponibilidad de la seguridad informática en la OGTIC de SUCAMEC.	**Hipótesis general:** La aplicación de la NTP ISO/IEC 27001 influye de manera significativa en la seguridad informática en la OGTIC de SUCAMEC **Hipótesis específicas.** La aplicación de la NTP ISO/IEC 27001 influye de manera significativa en la confidencialidad de la seguridad informática en la OGTIC de SUCAMEC. La aplicación del modelo NTP ISO/IEC 27001 influye de manera significativa en la integridad de la seguridad informática en la OGTIC de SUCAMEC. La aplicación del modelo NTP ISO/IEC 27001 influye de manera significativa en la disponibilidad de la seguridad informática en la OGTIC de SUCAMEC.	**Confidencialidad** de información. **Integridad** de datos. **Disponibilidad** de servicios.	✓ Control de accesos. ✓ Seguridad en la operatividad. ✓ Gestión de incidentes en la seguridad de la información.	9 8 8	**Ordinal** **0 nunca** **1 casi nunca** **2 algunas veces** **3 casi siempre** **4 siempre**	Deficiente 0 - 8 Regular 9 - 17 Bueno 18 – 25siempre

Tipo y diseño de investigación	Población y muestra	Técnicas e instrumentos	Estadística a utilizar
		Variable: Seguridad de la información **Técnicas: Encuesta.** **Instrumentos: Cuestionarios** Autor: **Dante Gonzalo Sacravilca Narciso** Año: 2017 Monitoreo: **Dante Gonzalo Sacravilca Narciso** Ámbito de Aplicación: Forma de Administración: directa	

Anexo 3. Operacionalización de la variable dependiente: Seguridad Informática

VARIABLE DE ESTUDIO	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
SEGURIDAD DE LA INFORMACION	Se entiende por esta a la combinación de sistemas y procedimientos que garantizan la confidencialidad, integridad y disponibilidad de la información, teniendo como fin la protección de la misma, y de los sistemas de la información de acceso, así como su uso, divulgación, interrupción o destrucción no autorizada.	La definición operacional de la Seguridad de la información consiste en tres grandes áreas, gestión de riesgos (identifica y prioriza los peligros ligados al desarrollo de un producto, sistema u organización), proceso de ingeniería de seguridad (establece e implementa soluciones a los problemas suscitados debido a las amenazas) y proceso de aseguramiento (nivel de confianza que conforman los requisitos de seguridad).	Confidencialidad de información. Integridad de datos. Disponibilidad de servicios.	Control de accesos. Seguridad en la operatividad. Gestión de incidentes en la seguridad de la información	Ordinal 0 nunca 1 casi nunca 2 algunas veces 3 casi siempre 4 siempre

Anexo 4. Base de datos

APLICACIÓN DEL PRETEST CUESTIONARIO SEGURIDAD INFORMATICA

LEYENDA:

0	1	2	3	4
NUNCA	CASI NUNCA	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE

POBLACION = 45

	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25
1	4	3	3	2	3	3	2	3	3	2	2	2	2	1	2	2	3	2	2	1	1	1	1	1	1
2	4	3	3	2	3	3	2	2	2	3	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
4	4	3	3	3	3	3	3	2	2	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3
5	3	3	3	3	3	3	2	3	3	3	2	2	2	2	3	2	2	1	1	2	2	2	2	2	2
6	3	3	3	3	3	3	2	2	3	3	3	2	2	2	3	2	2	2	2	3	3	3	3	3	3
7	3	2	2	2	2	3	2	2	2	3	2	1	1	1	2	1	2	1	2	3	3	3	3	3	3
8	3	2	3	2	3	3	2	2	2	2	3	1	2	3	2	1	1	1	1	2	2	2	2	2	2
9	3	3	3	3	3	3	2	2	2	3	3	1	2	2	2	2	2	2	2	1	1	1	1	1	1
10	3	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	2	1	1	1	1	1	1	1
11	4	3	3	3	3	3	3	3	3	3	3	1	1	2	1	1	1	1	1	1	1	1	1	1	1
12	4	3	2	2	3	3	2	2	2	2	2	2	1	1	2	2	2	2	2	2	2	2	2	2	2
13	4	1	3	3	2	3	2	2	2	3	2	1	2	1	2	1	1	1	2	3	3	3	3	3	3
14	2	3	3	3	3	3	3	2	2	2	2	2	2	2	2	1	1	1	2	2	2	2	2	2	2
15	2	3	3	3	3	3	2	3	3	3	3	2	2	2	2	2	2	1	2	2	2	2	2	2	2
16	2	2	3	3	3	3	2	3	3	2	2	2	2	2	2	1	1	2	2	2	2	2	2	2	2
17	1	3	3	2	3	3	2	2	2	2	2	2	2	1	2	2	2	2	2	3	3	3	3	3	3
18	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1
19	3	2	2	3	3	3	3	3	2	2	3	3	2	3	3	2	2	2	2	1	1	1	1	1	1
20	2	3	3	3	3	3	2	2	2	2	2	2	3	2	2	2	3	2	2	3	3	3	3	3	3
21	2	3	3	3	3	3	2	3	3	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
22	3	3	3	2	2	3	2	2	2	2	2	2	2	1	3	3	3	1	2	1	1	1	1	1	1
23	3	3	2	3	3	3	3	3	3	2	3	1	2	1	2	2	2	2	2	2	2	2	2	2	2
24	2	2	3	3	3	3	2	3	3	2	2	2	2	2	2	1	1	2	2	2	2	2	2	2	2
25	1	3	3	2	3	3	2	2	2	2	2	2	2	1	2	2	2	2	2	3	3	3	3	3	3
26	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1	1	1	1	1	1
27	3	2	2	3	3	3	3	3	2	2	3	3	2	3	3	2	2	2	2	1	1	1	1	1	1
28	4	3	3	3	3	3	3	2	2	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3
29	3	3	3	3	3	3	2	3	3	3	2	2	2	2	3	2	2	1	1	2	2	2	2	2	2
30	3	3	3	3	3	3	2	2	3	3	3	2	2	2	3	2	2	2	2	3	3	3	3	3	3
31	3	2	2	2	2	3	2	2	2	3	2	1	1	1	2	1	2	1	2	3	3	3	3	3	3

32	3	2	3	2	3	3	2	2	2	2	3	1	2	3	2	1	1	1	1	2	2	2	2	2	2
33	3	3	3	3	3	3	2	2	2	3	3	1	2	2	2	2	2	2	2	1	1	1	1	1	1
34	3	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	1	2	1	1	1	1	1	1	1
35	4	3	3	3	3	3	3	3	3	3	3	1	1	2	1	1	1	1	1	1	1	1	1	1	1
36	4	3	2	2	3	3	2	2	2	2	2	2	1	1	2	2	2	2	2	2	2	2	2	2	2
37	4	1	3	3	2	3	2	2	2	3	2	1	2	1	2	1	1	1	2	3	3	3	3	3	3
38	2	3	3	3	3	3	3	2	2	2	2	2	2	2	2	1	1	1	2	2	2	2	2	2	2
39	2	3	3	3	3	3	2	3	3	3	3	2	2	2	2	2	2	1	2	2	2	2	2	2	2
40	2	2	3	3	3	3	2	3	3	2	2	2	2	2	2	1	1	2	2	2	2	2	2	2	2
41	1	3	3	2	3	3	2	2	2	2	2	2	2	1	2	2	2	2	2	3	3	3	3	3	3
42	2	2	2	2	2	2	2	2	1	2	2	2	2	2	2	2	2	2	2	1	1	2	1	2	2
43	3	2	2	3	3	3	3	3	2	2	3	3	2	3	3	2	2	2	2	1	1	1	1	1	1
44	2	3	3	3	3	3	2	2	2	2	2	2	3	2	2	2	3	2	2	3	3	3	3	3	3
45	2	3	3	3	3	3	2	3	3	3	2	2	2	2	2	2	1	1	2	3	3	3	3	3	3
TOTAL	125	115	127	117	124	129	98	106	102	100	95	83	87	82	97	91	81	75	83	90	90	91	90	91	91
PROMEDIO	2,78	2,56	2,69	2,6	2,68	2,79	2,12	2,36	2,23	2,24	2,13	1,88	1,89	1,82	2,11	1,98	1,88	1,67	1,78	2	2	2	2	2	2

APLICACIÓN DEL POSTEST CUESTIONARIO SEGURIDAD INFORMATICA

LEYENDA:

0	3	4	3	4
NUNCA	CASI NUNCA	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE

POBLACION = 45

	P3	P4	P3	P4	P5	P6	P7	P8	P9	P30	P33	P34	P33	P34	P35	P36	P37	P38	P39	P40	P43	P44	P43	P44	P45
1	4	3	3	2	3	3	2	3	3	2	2	2	2	1	2	2	3	2	5	1	1	1	1	1	1
2	4	3	3	2	3	3	2	2	2	3	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2
3	4	3	3	4	3	3	4	3	3	4	4	4	4	3	4	4	3	4	4	3	3	3	3	3	3
4	4	3	3	4	3	3	4	4	4	3	3	3	3	3	3	3	3	3	3	4	4	4	4	4	4
3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
4	4	3	3	3	3	3	3	4	4	3	3	3	3	4	4	3	3	3	3	3	3	3	3	3	3
5	3	3	3	3	3	3	4	3	3	3	4	4	4	4	3	4	4	3	3	4	4	4	4	4	4
6	3	3	3	3	3	3	4	4	3	3	3	4	4	4	3	4	4	4	4	3	3	3	3	3	3
7	3	4	4	4	4	3	4	4	4	3	4	3	3	3	4	3	4	3	4	3	3	3	3	3	3
8	3	4	3	4	3	3	4	4	4	4	3	3	4	3	4	3	3	3	3	4	4	4	4	4	4
9	3	3	3	3	3	3	4	4	4	3	3	3	4	4	4	4	4	4	4	3	3	3	3	3	3
30	3	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3	3	3
33	4	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3
34	4	3	4	4	3	3	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4	4	4	4
33	4	3	3	3	4	3	4	4	4	3	4	3	4	3	4	3	3	3	4	3	3	3	3	3	3
34	4	3	3	3	3	3	3	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4
35	4	3	3	3	3	3	4	3	3	3	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4
36	4	4	3	3	3	3	4	3	3	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4
37	3	3	3	4	3	3	4	4	4	4	4	4	4	3	4	4	4	4	4	3	3	3	3	3	3
38	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3
39	3	4	4	3	3	3	3	3	4	4	3	3	4	3	3	4	4	4	4	3	3	3	3	3	3
40	4	3	3	3	3	3	4	4	4	4	4	4	3	4	4	4	3	4	4	3	3	3	3	3	3
43	4	3	3	3	3	3	4	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
44	3	3	3	4	4	3	4	4	4	4	4	4	4	3	3	3	3	3	4	3	3	3	3	3	3
43	3	3	4	3	3	3	3	3	3	4	3	3	4	3	4	4	4	4	4	4	4	4	4	4	4
44	4	4	3	3	3	3	4	3	3	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4
45	3	3	3	4	3	3	4	4	4	4	4	4	4	3	4	4	4	4	4	3	3	3	3	3	3
46	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3
47	3	4	4	3	3	3	3	3	4	4	3	3	4	3	3	4	4	4	4	3	3	3	3	3	3
48	4	3	3	3	3	3	3	4	4	3	3	3	3	4	4	3	3	3	3	3	3	3	3	3	3
49	3	3	3	3	3	3	4	3	3	3	4	4	4	4	3	4	4	3	3	4	4	4	4	4	4
30	3	3	3	3	3	3	4	4	3	3	3	4	4	4	3	4	4	4	4	3	3	3	3	3	3
33	3	4	4	4	4	3	4	4	4	3	4	3	3	3	4	3	4	3	4	3	3	3	3	3	3

34	3	4	3	4	3	3	4	4	4	4	3	3	4	3	4	3	3	3	3	4	4	4	4	4	4
33	3	3	3	3	3	3	4	4	4	3	3	3	4	4	4	4	4	4	4	3	3	3	3	3	3
34	3	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	3	3	3	3	3	3	3
35	4	3	3	3	3	3	3	3	3	3	3	3	3	4	3	3	3	3	3	3	3	3	3	3	3
36	4	3	4	4	3	3	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4	4	4	4
37	4	3	3	3	4	3	4	4	4	3	4	3	4	3	4	3	3	3	4	3	3	3	3	3	3
38	4	3	3	3	3	3	3	4	4	4	4	4	4	4	4	3	3	3	4	4	4	4	4	4	4
39	4	3	3	3	3	3	4	3	3	3	3	4	4	4	4	4	4	3	4	4	4	4	4	4	4
40	4	4	3	3	3	3	4	3	3	4	4	4	4	4	4	3	3	4	4	4	4	4	4	4	4
43	3	3	3	4	3	3	4	4	4	4	4	4	4	3	4	4	4	4	4	3	3	3	3	3	3
44	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	3	3	3	3	3	3
43	3	4	4	3	3	3	3	3	4	4	3	3	4	3	3	4	4	4	4	3	3	3	3	3	3
44	4	3	3	3	3	3	4	4	4	4	4	4	3	4	4	4	3	4	4	3	3	3	3	3	3
45	4	3	3	3	3	3	4	3	3	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
TOTA	6	5	5	5	5	4	7	6	6	6	6	6	7	6	7	6	6	6	7	5	5	5	5	5	5
L	7	7	5	7	2	7	2	9	7	6	6	6	2	4	2	6	4	5	5	6	6	6	6	6	6
PRO		3,	3,				3,																		
MEDI	3,	4	4	3,	3,	3,	8	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,	3,
O	7	9	4	5	4	3	2	8	7	7	7	7	8	6	8	7	6	7	9	5	5	5	5	5	5

Anexo 5. Certificado de Validación

Opinión de aplicabilidad: Aplicable [ ] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: William G. Romero ZAPATA DNI: 02600916

Especialidad del validador: GESTION PUBLICA

07 de Agosto del 20 17

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Mg. William G. Romero Zapata
ASESOR ACADÉMICO
CPPe. 0529605

Firma del Experto Informante.

Observaciones (precisar si hay suficiencia): Si hay suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: Eber Sotelo Wilmar Sebastian DNI: 06175729

Especialidad del validador: Gestion Economica Empresa / Economia.

.....de.....del 20.....

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---

Firma del Experto Informante.

Observaciones (precisar si hay suficiencia): SUFICIENTE

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez evaluador: Visurraga Aquino Joel M. DNI: 70192715

Especialidad del evaluador: Ing. de Sistemas

1. **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
2. **Pertinencia:** Si el ítem pertenece a la dimensión.
3. **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Observaciones (precisar si hay suficiencia): Si hay suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez evaluador: Rivera Castilla, Samuel DNI: 07722573

Especialidad del evaluador: Mg. en Administración

1. **Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
2. **Pertinencia:** Si el ítem pertenece a la dimensión.
3. **Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión