UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIOS DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023

Tesis para obtener el título profesional de Ingeniero en Informática y de Sistemas

Autor

Gonzales Torres Jackson Junior

Asesor

Wilmer Carrasco Alvarado

Código ORCID 0000-0003-3138-9808

Huaraz – Perú

2023

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

PALABRAS CLAVE:

Tema	Seguridad Informática
Especialidad	Sistemas de información

KEYWORDS:

Theme	Security Policy
Specialty	Information System

LÍNEA DE INVESTIGACIÓN:

Línea	Sistema de Seguridad
Área	Ciencias Sociales
Sub Área	Economía y Negocios
Disciplina	Negocios y Management

CONSTANCIA DE ORIGINALIDAD

El que suscribe, Vicerrector de Investigación de la Universidad San Pedro:

HACE CONSTAR

Que, de la revisión del trabajo titulado **"Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023"** del (a) estudiante: **GONZALES TORRES JACKSON JUNIOR**, identificado(a) con Código Nº **1411100037**, se ha verificado un porcentaje de similitud del **21%**, el cual se encuentra dentro del parámetro establecido por la Universidad San Pedro mediante resolución de Consejo Universitario Nº 5037-2019-USP/CUpara la obtención de grados y títulos académicos de pre y posgrado, así como proyectos de investigación anual Docente.

Se expide la presente constancia para los fines pertinentes.

Chimbote, 18 de diciembre de 2023

UNIVERSIDAD SAN PEDRO
VICERRECTORADO DE INVESTIGACIÓN
Dr. JAVIER MARTÍNEZ CARRIÓN
VICERRECTOR

NOTA: Este documento carece de valor si no tiene adjunta el reporte del Software TURNITIN.

Urbanización Laderas del Norte H-11
Teléfono: 043 – 483070
vicerrectorado.investigacion@usanpedro.edu.pe
https://investigacion.usanpedro.edu.pe

TÍTULO

Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023

RESUMEN

Este estudio se trazó el objetivo general determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash, la hipótesis consistió en el Plan de mejora influye positivamente en la seguridad de la información. La investigación fue no experimental, transversal y descriptivo. Trabajó con población de 123 usuarios y muestra de 29 usuarios del sistema de información. Se aplicó la técnica de observación, análisis y encuesta, el instrumento fue el cuestionario. Se concluyó que el Plan de mejora influyó en un 22.09% en la seguridad de la información. La diferencia media de las frecuencias antes y después en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial fue 0.48, esto significó que tuvo influencia en la mejora de la seguridad de la información en 28.00%. La diferencia media de las frecuencias antes y después en la gerencia Regional de Desarrollo Económico fue 0.41, esto significó que tuvo influencia en la mejora de la seguridad de la información en 23.53%. La diferencia media de las frecuencias antes y después en la Gerencia Regional de Desarrollo Social fue 0.28, esto significó que el plan de mejora de seguridad de la información tuvo influencia en la mejora de la seguridad de la información en 14.81%. La diferencia media de las frecuencias antes y después en la Gerencia Regional de Infraestructura fue 0.38, esto significó que hubo influencia en la mejora de seguridad de la información en 22.09%.

ABSTRACT

The general objective of this study was to determine to what extent the Improvement Plan applying the ISO/IEC 27001 standard influences information security in the Regional Government of Ancash, the hypothesis consisted of the Improvement Plan positively influences information security. The research was non-experimental, cross-sectional and descriptive. It worked with a population of 123 users and a sample of 29 users of the information system. The observation, analysis and survey technique were applied, the instrument was the questionnaire. It was concluded that the Improvement Plan had a 22.09% influence on information security. The mean difference between the frequencies before and after in the Regional Management of Planning, Budget and Territorial Conditioning was 0.48, This meant that it had an influence on improving information security by 28.00%. The mean difference of the frequencies before and after in the Regional Economic Development management was 0.41, this meant that it had an influence on the improvement of information security by 23.53%. The mean difference between the frequencies before and after in the Regional Management of Social Development was 0.28, this meant that the information security improvement plan had an influence on the improvement of information security by 14.81%. The mean difference between the frequencies before and after in the Regional Infrastructure Management was 0.38, which meant that there was an influence on the improvement of information security in 22.09%.

I. INTRODUCCIÓN

La seguridad del sistema de informacion y los activos informáticos son aspectos muy importantes para toda organización pública o privada, en ese sentido, el presente estudio busca alcanzar un Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023, con la finalidad de conocer el estado situacional de los conocimientos de las variables en estudio, se ha analizado los antecedentes locales, nacionales e internacionales con el proposito de discutirlos y compararlos con los resultados de esta investigación.

A nivel internacional, Baldeón (2021) en la tesis de grado realizada en la Universidad Regional Autónoma de los Andes, Ecuador; se planteó el objetivo de realizar el desarrollo de un plan Informático fundamentado en ISO/IEC 27001:2013 con la finalidad de mejorar la calidad relacionados con los temas de seguridad de la información. Elaboró investigación mixta, descriptiva no experimental, aplicó investigación bibliográfica y de campo, y métodos deductivo e inductivo, trabajó con 50 personas entre adminsitrativos, docentes y estudiantes como parte de toda la población, aplicó encuesta y entrevista. Tuvo como resultado que el 94% de los encuestados opinaron que necesitaban mejorar los problemas implicados con los temas de la seguridad de la información, el 26% indicaron que existe plan de contingencia, el 74 que no existe el pan de contingencia. Concluyó la implementación de ISO/IEC 27001:2013 favoreció la disminución significativa de costos, así como también, mejorar muchos aspectos del funcionamiento de los procesos internos de los procesos de seguridad.

Mendoza (2019) en la tesis de grado realizada en una universidad estatal colombiana de tipo distancia y abierta; se planteó el objetivo de realizar el diseño del Sistema indicado fundamentado en NTC ISO/IEC 27001 con el propósito principal de garantizar aspectos de seguridad a la información en sus dimensiones clásicas de confianza o confidencialidad, integridad de la información y su

respectivo acceso conocido como disponibilidad. Aplicó metodología mixta, de tipos descriptiva y exploratoria, aplicó entrevista, encuestas, lista de chequeo; la población estuvo conformada por funcionarios, la muestra fue de tamaño de 72 funcionarios. Tuvo como resultado que encontró 637 amenazas con impactos calificados como moderado, alto y muy alto. Concluyó que con la instrumentalización de la norma indicada y trabajada se pudo evidenciar que fue urgente la deficiencia en la implantación del Sistema de Gestión de Seguridad de la información para la institución.

Alban (2018) en la tesis de grado desarrollada en la Universidad Regional Autónoma de Los Andes, Ecuador; se trazaron el objetivo de realizar el perfeccionamiento de un Plan de seguridad informática fundamentado en el estándar internacional ISO/IEC 27001-2013 con la finalidad de realizar mejoras en las características importantes de la seguridad de los archivos de información generados en la institución como consecuencia de labores administrativas y operativas en el espacio indicado. Emplearon investigación con método inductivo y deductivo, realizaron análisis y método sintético, hipotético deductivo, investigación directamente en el objeto de estudio y de forma bibliográfica, el estudio fue aplicado, descriptivo cuantitativo, la población muestral estuvo conformada por 7 personas, aplicó encuesta y entrevista. Concluyó que el plan informático fue desarrollado en función a los requerimientos muy importantes de tipo operativas y administrativas de la institución, y que contribuyó en mejorar la seguridad de los procesos llevados a cabo de manera adecuada, sistematizada y correcta con los controles y los compromisos de la defensa y cuidado de los activos más importantes como fueron la información de cualquier ataque, riesgo y vulnerabilidades. Concluyó que ISO 27001:2013 contribuyó en la mejora de la seguridad de los bienes o activos informáticos y los recursos tecnológicos.

Simbaña (2018) en la tesis realizada en la Universidad Regional Autónoma de Los Andes, Ecuador; se trazó el objetivo de aplicar un diseño de un plan informático fundamentado en ISO/IEC 23001:2013 con fines de mejora de la Seguridad de los

activos informáticos, infraestructura y recursos tecnológicos. Aplicó métodos de inferenciacion con deducción e inducción, analítico y sintético, investigación con toma de datos en campo y bibliográfica, el estudio fue no experimental, descriptivo cuantitativo, aplicó encuesta y entrevista. Concluyó que la unidad educativa no tuvo un área específica de informática, que se tuvo que organizar los documentos en calidad de regulatorios para que brinden una normativa y responsabilidades, con ello se va a garantizar a que los usuarios sean ubicados o asignados por sus actividades. Se va a establecer políticas y normas de seguridad con fines de perfeccionar la seguridad de la información y los medios tecnológicos. El plan de contingencia va ayudar en la determinación de probables riesgos relacionados con la infraestructura tecnológica, para ello propuso el plan preventivo. Que el plan desarrolado en el periodo 2018-2022 basado en el estándar normativo internacional indicado va a perfeccionar la seguridad de la información, las instalaciones tecnológicas en el objeto estudiado.

A nivel nacional, Abanto (2023) en la tesis de grado elaborada en la universidad estatal huanuqueña; abordó el objetivo de efectuar a modo de propuesta un modelo enfocado en la gestión sistémica de seguridad de los activos de información sustentado en la NTP ISO/IEC 27001:2014 con la finalidad de mejorar la seguridad de la información en el espacio estudiado. Trabajaron al estudio como tipo de investigación tecnológica, diseño cuasi experimental con enfoque cuantitativo, trabajaron con una población 500 activos fiscos y 200 empleados de la institución pública, mientras que la muestra estuvo conformada por 1000 activos y 74 funcionarios, aplicaron guía y ficha de entrevista. Tuvo como resultado que estaban aplicando la norma con un 0% del cumplimiento de la norma indicada, en función a ello, tuvieron que elaborar el modelo propuesto fundamentado en función a lo estipulado en la norma indicada el espacio en que fue realizado la gestión de riesgo con todos los controles implicados controles. Determinaron que existió relación con la seguridad en las dimensiones lógica y física del objeto estudiado. Evaluaron la amenaza, vulnerabilidad y los riesgos que pudieron estar presentes y exponer a todos los activos, específicamente los de tecnología informática bajo la norma

indicadas y aplicadas. Concluyeron que la propuesta del modelo de seguridad de la información basado en la norma aplicada se pudo evidenciar procesos de mejora de la seguridad de la información en un 23.6%.

García (2020) en la tesis de grado "desarrollada en la Universidad Católica Los Ángeles de Chimbote, Perú; se planteó el objetivo de llevar a cabo un sistema de gestión de seguridad informática cimentado en el estándar internacional ISO 27001 en el espacio estudiado. Aplicó metodologia Magerit y Octave, el enfoque utilizado fue de trabajo con datos numéricos, es decir, trabajó con datos numéricos, de nivel descriptivo, con diseño de no manipulación de variable, lo cual significó no experimental, la población estuvo estructurada con 23 trabajadores y la muestra con el mismo tamaño de elementos de muestra, aplicó técnica de la encuesta y cuestionario. Encontró que el 91.00% indicaron que no se estaba brindando seguridad de la información y que el 9.00% señalaron que si se brindaba seguridad a los activos de información. El 87% de participantes presentaron conocimientos adecuados en el uso de la norma ISO 27001, mientras que el 13% no presentaron esos conocimientos, el 96% indicó que, si demostraron un cierto nivel de cultura en la adecuación, control y monitoreo de los protocolos de seguridad de la información, y el 4% indicaron que no lo realzaban. Concluyó que se evaluó el estado situacional de cada uno de los procesos de seguridad en función al estándar internacional estudiado, debido a ello, se pudo establecer los inconvenientes presentados relacionados con la seguridad de la información. Que los marcos de referencia contribuyeron en realizar la propuesta de mejoras en la seguridad. Concluyó se realizó la propuesta de la aplicación de la Norma aplicada con la finalidad de mejorar la seguridad en el espacio estudiado.

Poma (2019) en la tesis de grado realizada en la Universidad Privada Antenor Orrego, Perú; se planteó el objetivo de desarrollar el diseño de un plan de seguridad de la información en función a la norma ISO/IEC 27001 con fines de mejorar la gestión de la seguridad de la información. Trabajó investigación sin manipulacion de variables, es decir, no experimental, cuyo nivel fue descriptiva, aplicó evaluación

y control, análisis y elaboración del plan. Concluyó que de acuerdo a los problemas encontrados se presentó la necesidad de realizar la propuesta de la elaboracion del plan de mejora de la seguridad de la información fundamentada en la norma internacional estduiada y aplicada en la investigación. Que la elaboración del Plan de Seguridad aportó de manera muy significativa en el procesos de perfeccionamiento de la seguridad de la información, esta mejorar consistió en lograr un pefeccioanmiento de la dimensión confidencialidad en 17.59%, respecto a la dimensión disponibilidad fue 30.51% y en la dimensión integridad fue 14.66%. Que la propuesta va a aportar para la institución con la emisión de sugerencias con la finalidad de darle la importancia debida a los procesos y tareas que se debieron realizar y considerar durante la etapa de analisis y evaluación adecuada del Sistema de Control Interno, así como en las actualizaciones futuras.

A nivel local, Guardia (2020) en la tesis de maestría se trazó el objetivo de realizar el diseño de un modelo de seguridad de la información cuyo propósito fue reducir los riegos informáticos en el objeto de estudio. Trabajó investigación aplicada, tipo de investigación implicó determinar relacion, por lo que fue de tipo correlacional, mientras que el enfoque fue cuantitativo debido a que se trabajó con datos numéricos, explicativo y propositivo, de diseño experimental longitudinal; aplicó ficha de recolección de datos y ficha resumen. Encontró que las necesidades importantes relacionados con los temas de seguridad de la información del sistema en el antes fue 83% y después 95%, los trabajadores que conocen la política seguridad fueron 0.05% y 1005, los que cumplieron con la seguridad fueron 1% y 90%, las vulnerabilidades fueron 40% y 90%, los riesgos altos fueron 0% 0% y 38%. Concluyó que el modelo de seguridad de la información permitió el logro de minimizar los riesgos de seguridad de la información, logró optimizar riesgos de los activos admitiendo conocer que equipos de TI estaban disponibles y operativos. Concluyó que el personal fue crítico en el proceso de sensibilización respecto a la seguridad informática, con el modelo, el personal fue consciente que la información fue muy importante en los aspectos de confidencialidad, en integridad y accesibilidad, que las amenazas estuvieron presentes con frecuencia, lo cual estuvo

generando vulnerabilidad con riesgos probables de afectar a la seguridad. El modelo propuesto permitió implementar mecanismos y controles de reducción de los riesgos a niveles mínimos.

Los fundamentos teóricos de la seguridad de la información, las instituciones gubernamentales como los gobiernos regionales disponen de grandes sistemas de información y comunicación que le permite desarrollar sus procesos operativos y administrativos en función a las normas internas establecidas, en estos procesos, reciben y generan diversos tipos de información que son almacenados como archivos lógicos y físicos, una buena cantidad de estos archivos tienen un gran valor para la institución, y tienen la característica de ser confidenciales porque, en un determinado tiempo, el contenido mensaje solo deben conocer el personal autorizado, y no otras personas, incluso personal de la institución; estos archivos pueden ser, archivos de licitaciones de obras, archivos de acuerdos tomados por la alta gerencia, y cualquier otro archivo que la institución considere como de alta importancia; estos archivos deben ser protegidos para garantizar, que ciertos procesos que realiza el estado, se deban realizar con lo estipulado de acuerdo a ley, ninguna persona natural o jurídica debes saber su contenido hasta un cierto tiempo, esto es para que se cumplan ciertas características de legalidad e igualdad de participación de las empresas proveedoras de servicio en las licitaciones (Samaniego y Ponce, 2021; Hamid, 2007).

Para que las instituciones puedan proteger sus activos de tipo físico y lógico, deben adoptar políticas de seguridad con la finalidad de garantizar Un determinado nivel de protección de los activos informáticos contra cualquier tipo de amenaza, buscar que se disminuyan los riesgos de ataques, los cuales pueden provenir de agentes internos o externos; estas políticas van acompañadas de normas nacionales e internacionales. la seguridad de la información se garantiza con la concientización, la adquisición de habilidades, capacidades y competencias y la aplicación de estas al momento de hacer frente cualquier tipo de riesgo o ataque a

la que se puede enfrentar los usuarios del sistema de información (Smith, 2019; Miguel, 2015).

Política de seguridad. La implementación de una política de seguridad consiste en establecer directivas, estándares, guías, buenas prácticas y procedimientos que van a normal las actividades desarrolladas por los usuarios de un determinado sistema de información, la política de seguridad implica el establecimiento de técnicas, responsabilidades y métodos, así como, consideraciones y buenas prácticas que deben de adquirir todos los usuarios del sistema de información. Una buena política de seguridad consiste en hacer uso del sistema de forma segura, utilizarla solo para los casos de la institución, y que el personal debe estar plenamente consciente de la importancia de la seguridad informática, por lo tanto, de estar preparado de forma continua, tanto en el uso del sistema, como para hacer frente cualquier tipo de ataque informático proveniente de agentes internos o externos Mohamed, 2019; Mercado, 2016).

De acuerdo con la literatura científica, las políticas de seguridad, tiene como función cumplir con caracterizar la imagen externa de la institución, esto se da cuando, la política establecida, tiene efectos positivos en toda la institución, y estos efectos se reflejan en la sociedad, por lo tanto, la sociedad califica el desempeño de esta organización en función a lo alcanzado como derivación de la implantación de la política de seguridad (Chicano, 2014; Vidalina, 2012).

Principios básicos de la seguridad de la información: Los pilares fundamentales de la seguridad indicada consiste en cuidar las principales atributos o dimensiones de dicha información, estos son, la confianza expresada en confidencialidad, que el archivo debe estar completo o integro, así como también que tiene que estar disponible o accesible, también conocido como disponibilidad. Toda la información que genera una institución se constituye como un activo fundamental y de mucho valor, la información puede ser desarrollada o generada dentro o fuera de la institución. En función al valor, toda información tiene

jerarquía, tanto en importancia como valor para la institución, mientras más valor tenga la información, mayor será el interés de los agentes internos y externos de poder apropiarse y afectar sus dimensiones de integridad, accesibilidad y confidencialidad (Tupia, 2010).

Una información es confidencial cuándo, de acuerdo a las normas de la organización, solo un grupo de personas puede conocer el contenido mensaje de la información, cuando un atacante, interno o externo, accede a una información para conocer su contenido, que está violando la confidencialidad del activo (INCIBE, 2019; AENOR, 2014). La integridad de un activo informático, dicho activo está completo y que no ha sido variado, en este caso el activo se muestra tal cual es; la violación de la integridad de un documento indica que un atacante interno o externo, se ha apropiado o mutilado una parte de la información dejando al archivo original incompleto. la dimensión accesibilidad hace referencia a que los archivos o activos de información deben estar siempre disponibles para quién es tienen los privilegios de acceder, un atacante puede hacer te usuario creador del activo informático no pueda acceder a su propio archivo, en este caso se ha violado el principio de la accesibilidad del bien informático (Romero et al, 2018).

Metodología para mejorar la seguridad de la información. En la presente investigación se va a aplicar la metodología de mejora continua de planificar, hacer, verificar y actuar (PHVA) también conocido por su acrónimo en inglés Planning, Do, Check y Act (PDCA) y el Estándar ISO/IEC 27001 (Mora, 2020; ISO/IEC, 2016).

Ciclo de mejora continua: Los sistemas de información, en cuanto a tecnología, cada cierto periodo de tiempo va evolucionando, esto significa que ciertas características adoptan capacidades superiores, ya sean en capacidad de almacenamiento, velocidad de procesamiento, nuevos programas que deben ser aprendidos y aplicados, nuevos sistemas de virus que deben ser enfrentados y repelidos, etc. Así como mejora la tecnología, también mejora, poder mejorar la

seguridad informática en la organización de forma continua. Generalmente las empresas que desean mejorar la seguridad de la información aplican el ciclo de mejora contínua conocido por sus siglas PHVA (Costas Santos, 2004).

Al ciclo PHVA o PDCA lo conceptúan como metodología enfocada en los procesos de mejora continua que contiene cuatro fases o etapas, que implica desarrollar trabajos de planificación, ejecutar actividades, verificar o controlar y actuar, las etapas de este ciclo son los siguientes (Gómez, & Fernández, 2015; ISO2700.es. 2012):

Plan. La fase plan del PDCA se encarga de la realización de la planificación cuyo objetivo consiste en la implantación del sistema en función a la seguridad Relacionado con la información, conlleva realizar el análisis del contexto de la institución, establecer precisamente las metas y los objetivos, seguido de las políticas con un enfoque de alcanzar los objetivos y metas planificadas. En esta fase también se instauran las actividades y tareas que necesariamente tienen que realizarse o llevarse a cabo para implantar el sistema de la seguridad de cada uno de los espacios deseados.

Do. En la fase de hacer se trata de poner en funcionamiento el sistema de seguridad del sistema de información de la institución, esto conlleva en poner en práctica todos los controles y las políticas establecidas con el propósito fundamental de monitorear o fiscalizar los riesgos, aplicar y disponer actividades y procesos que van a conllevar a la caracterización de los riesgos y tipos de riesgos. La fase de hacer consiste en la ejecución de todas las actividades que han sido planificadas, y que van a ser realizadas por el personal que también ya ha sido asignado para el desarrollo de estas tareas.

Check. En esta fase de la mejora continua se realiza el desarrollo del monitoreo o verificación, así como también la fiscalización que se va a llevar a cabo como parte del plan de seguridad del sistema de información institucional. La verificación trata de controlar cada uno de los procesos de actividades para que sean aplicadas tal como han sido establecidas, y cada una de las objetivos y metas deben estar

cumpliéndose, tal como han sido establecidos dentro de los indicadores de eficiencia y eficacia (Mora, 2020; Calder, 2009).

Act. En la fase de actuar de esta metodología, se trata de mejorar y mantener una mejora contínua relacionado con la seguridad de la información, en ese sentido, los participantes deben de definir y ejecutar Todas las acciones correctivas que han sido evidenciados con el objetivo de minimizar riesgos, peligros y vulnerabilidades. Ese café ejerce una función de control de todo lo actuado en las 3 etapas anteriores, por lo tanto, es de vital importancia cuando se quiere asegurar la mejora continua de cualquier actividad desarrollada en la institución en función a la seguridad del Sistema de información (ISO/IEC, 2016).

Ciclo PDCA y su aplicación en el Gobierno regional

En la fase de actuar de esta metodología, se trata de mejorar y mantener una mejora contínua relacionado con la seguridad de la información, en ese sentido, los participantes deben de definir y ejecutar todas las acciones correctivas que han sido evidenciados con la finalidad de reducir los riesgos, peligros y vulnerabilidades. Ese café ejerce una función de control de todo lo actuado en las 3 etapas anteriores, por lo tanto, es de vital importancia cuando se quiere asegurar la mejora continua de cualquier actividad desarrollada en la institución en función a la seguridad del Sistema de información (PORTANTIER, 2013).

En la fase de planeación, hacer, verificar y actuar se debe realizar las siguientes actividades para el caso del Gobierno regional de Ancash:

Planear. En esta fase se tiene que: Definir y establecer el alcance del sistema de gestión de seguridad de la información. Establecer apropiadamente la política de seguridad que van a contribuir a que los elementos del Sistema de información funcionen de manera segura. definir qué metodología será utilizada en cuanto a la valoración de cada uno de los riesgos de seguridad encontrados. Identificar los riesgos por cada unidad o área del Gobierno Regional. Analizar profundamente y evaluar metódicamente los riesgos que se han encontrado. Establecer las estrategias

para el tratamiento de cada uno de los riesgos. Seleccionar aquí control de se van a aplicar Para cada riesgo. Por último, definir la aplicabilidad fundamentada en los controles escogidos para los riesgos de seguridad (Mora, 2020).

Hacer. Este nivel abarca: Establecer una definición clara y concisa de la definición del plan de tratamiento de riesgos de seguridad de la información. Ejecutar de forma metodológica y sistemática el plan de tratamiento de riesgos de acuerdo con las normas y políticas establecidas. Aplicar los controles establecidos y seleccionados. Establecer un método de medición de indicadores para medir los resultados. Revisar la ejecución del plan de concientización y formación de los colaboradores. Desarrollar la gestión de las operaciones o de los aspectos operativos que implican la seguridad de la información. Revisar adecuadamente la gestión de cada uno de los recursos. Revisar los procedimientos de detección y atención oportuna de riesgos e incidentes de seguridad potenciales y presenciales (Smith, 2019, Alexander, 2007).

Verificar. Para esta fase la institución debe de efectuar las siguientes acciones: Revisar y monitorear cada uno de los riesgos que se presenten en las unidades o áreas de la institución. Realizar las mediciones efectivas de los controles que son implementados. Evaluar los riesgos, así como también los niveles con que han sido aceptados. Las actividades también deben ser realizadas por la alta dirección de la Institución gubernamental. Realizar los procesos de actualización de los planes de seguridad de información. Llevar un registro de las acciones de la mejora de la seguridad de la información en función al rendimiento del sistema (Rodríguez & Peralta, 2019).

Actuar. Para esta última fase la institución debe de efectuar las siguientes acciones: Aplicar mejoras relacionada con los riesgos de la seguridad de la información y que garanticen su sostenibilidad por un tiempo prudencial aceptado por la misma institución. Desarrollar acciones correctivas y preventivas, sí, es necesario también, acciones predictivas. Informar el impacto de las mejoras y las

posibilidades de seguir mejorando En relación a la seguridad de la información (Chicano, 2015).

Estándar ISO/IEC 27001: Es un estándar mundial que ha sido desarrollado para facilitar a las empresas y organizaciones del mundo para que puedan realizar actividades y procesos con la finalidad de garantizar la seguridad de los sistemas de información, este estándar de seguridad guía, orienta y recomienda sobre cómo desarrollar la implementación las operaciones, el monitoreo, mantenimiento y mejora con relación a la Gestión de Seguridad de los sistemas de información. Contribuye a las instituciones en el establecimiento de políticas, metas y objetivos relacionados con la seguridad de la información, así como también, en entender los procesos de gestión de seguridad de la información, establecer objetivos pertinentes y de acuerdo a la realidad del sistema de información disponible; ayuda a la revisión periódica de los cumplimientos de la seguridad de la información, ayuda en la adopción de una perspectiva holística e integral de las seguridad de la información, este estándar ha sido diseñado para demostrar compatibilidad y armonía con otras normas internacionales, eso garantiza su integración (Mora, 2020; Baca, 2016).

El estándar ISO 27001 alcanza instrucciones tecnológicas para garantizar la seguridad de la información, genera un conjunto de conocimientos para poder desarrollar buenas prácticas del uso del sistema de información en función a la seguridad de todo el sistema, este estándar recomienda que los usuarios de las tecnologías de la información puedan adoptar una disciplina sobre cómo usar cada elemento tecnológico y, en función a ello, asegurar un uso metodológico correcto y adecuado Para garantizar el uso eficiente de las herramientas tecnológicas (Gómez & Fernández, 2015). Esta norma establece una cantidad de requisitos que se debe tener en cuenta para desarrollar una adecuada gestión de la seguridad de la información (Calder, 2009).

ISO 27001 alcanza todas a todas las instituciones públicas y privadas un punto de vista panorámico sobre la seguridad informática es generada por medio de un

sistema tecnológico, aborda los temas de cómo se deben desarrollar y trabajar los sistemas de gestión de seguridad de la información, este estándar describe los fundamentos de este tipo de sistemas usando los términos apropiados para que cualquier institución pueda adoptarlo como una norma de uso de los sistemas de información (Borja, 2018; Berrio, 2016). Este estándar también es considerado como un manual de buenas prácticas relacionados con la seguridad de los activos informáticos (Chicano, 2015).

El objetivo principal de la norma ISO 27001 consiste en que cada usuario del sistema informático institucional pueda adoptar conductas básicas sobre el uso en la forma correcta y esperada las tecnologías informáticas, así como también, busca garantizar la seguridad fundamental de los activos de información en las dimensiones de integridad, confidencialidad y disponibilidad (ISO/IEC, 2016).

La utilidad de este estándar internacional consiste en diagnosticar el estado situacional de los activos de un sistema de información mediante la técnica de la entrevista, para luego desarrollar un estudio analítico bastante profundo de los riesgos a los que pueden estar disponibles los activos informáticos. Este estándar también se puede utilizar para diseñar un plan de acción relacionados con la seguridad de los activos informáticos de la institución, así como también, diseñar las actividades y procesos y, conocer la cantidad de los requerimientos que se va a utilizar en la seguridad (ISACA, 2009).

Fases de aplicación de ISO 27001. Este estándar internacional de seguridad en el uso de los sistemas de información presenta cuatro fases para su aplicación, Esta fase es conocida como el ciclo de Deming, Y consiste en planificar, Implementar, Controlar Hoy y actuar Para perfeccionar de forma contínua al sistema de gestión de seguridad enfocada al cuidado de los archivos de información (Alvarado, 2016).

Planificación: Inicia el proceso de fase de inicio, que consiste en planificar de manera integral, la implantación del sistema de gestión de seguridad informática.

Esta fase se inicia con la idea de planificación de objetivos de seguridad de la información, se analizan los riesgos, vulnerabilidades y peligros que pueda tener los activos informáticos, se instituyen las políticas, procesos y conjunto de actividades coherentes con el establecimiento de la seguridad de la información, implica la organización de quienes van a realizar las tareas Para cumplir con los objetivos planteados y garantizar la seguridad estudiada (Borja, 2018).

Implementación: Esta fase se inicia con la implantación de un plan de tratamiento de los riesgos que podrían afectar al sistema de información y a los activos informáticos, en esta fase se toman todas las medidas preventivas para evitar eventos o situaciones que puedan dañar, tanto el Sistema de información como los activos informáticos, la protección a los riesgos en esta fase se trata de la perspectiva física y lógica, lo cual significa que se deben proteger los activos físicos y la parte de programación, información digital y software. La fase de implementación involucra poner en marcha los procesos de detección y respuesta a incidentes de seguridad, es la operación de lo planificado en función a procesos, política, controles y procesos del sistema de seguridad estudiada (Alvarado, 2016; Vidalina, 2012).

Fase de control o de verificación: En esta fase se controlan todos los procesos realizados en la fase anterior, consiste en realizar el monitoreo del funcionamiento del sistema y control de todas las unidades o elementos que conforman el Sistema de información, el control se puede realizar mediante observación, análisis y aplicación de auditorías interna y externa. Esta fase es un proceso de evaluación y comparación de cómo se está realizando la implementación del sistema de seguridad de la información comparado con los objetivos y políticas establecidas, involucra evaluación del control de las actividades realizadas, finalmente está en la función de elaborar un informe sobre lo controlado o evaluado (Migga, 2020; Llontop, 2018).

Actuación, mantenimiento y mejora: La fase de actuación consiste en dar un tratamiento de mejora a las actividades o procesos que se han considerado como que no satisfacen las políticas establecidas con los procesos que no están cumpliendo con garantizar un conveniente control de la seguridad informática, implica encontrar a riesgos o factores que ponen en peligro la seguridad de información y tomar las acciones correctivas, así como también informar sobre los resultados encontrados y las acciones que se han realizado para poder mejorar las irregularidades encontradas. Esta fase se fundamenta en los resultados obtenidos en una auditoría o evaluación interna, esto significa que lo que se va a mejorar las deficiencias que han sido detectadas mediante un proceso oficial de evaluación o auditoría (Migga, 2020).

Cuando cualquier institución desee implementar el estándar ISO 27001, debe aplicar las fases del ciclo de Deming, el cumplimiento de la realización de todas estas fases va a garantizar que la seguridad de la información cumpla con ciertos niveles de Protección de riesgos y cumplimiento de estándares de seguridad.

Dimensiones de la seguridad de la información. Para propósitos de este estudio, se ha tomado como dimensiones de la seguridad de la información a la gestión de riesgos y a la gestión de seguridad. La gestión de riesgos tiene como indicadores a los riesgos que se pueden encontrar en el software, riesgos de hardware, y riesgos en los activos informáticos. La dimensión gestión de seguridad tiene como indicadores al proceso de identificación de riesgos, al proceso de identificación de vulnerabilidades, nivel de conocimiento de ataques por parte de usuarios y, nivel de protección que necesario pueden dar al sistema de información. Todos estos procesos deben ser gestionados para garantizar la seguridad de la información (Llontop, 2028)

Gobierno Regional: El Gobierno regional de Áncash es una institución gubernamental creada por ley, sus gobernantes son elegidos por elección o voto popular, tiene como función administrar todos los requerimientos de la población

que se encuentra dentro de su espacio jurisdiccional, para ello dispone de un presupuesto que está constituido por ingresos propios Ingresos que les provee el Gobierno central.

La presente investigación es justificada en el aspecto social debido a que con el plan de mejora de la seguridad estudiada utilizando el estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, cada uno de los usuarios de esta institución gubernamental va a adquirir las habilidades, capacidades y competencias, así como las técnicas y metodológicas de cómo aplicar este estándar internacional de seguridad en información. Los beneficiarios directos van a ser los trabajadores o colaboradores del Gobierno regional, los usuarios que cada día se atienden en esa institución, y la misma institución en su conjunto.

Asimismo, el presente estudio se justifica en el plano económico porque con el plan de mejora de seguridad de la información que se va a implementar, se van a reducir los riesgos de la seguridad de la información, se van a evitar pérdidas de información y tiempo, y como consecuencia de ello, se dan evitar costos innecesarios ocasionados por pérdida de información, reparación de activos informáticos, reparación de hardware, asignación de personal especializado a resarcimiento de los daños que pueda causar la exposición a los riesgos en los sistemas informáticos.

Asimismo, el presente estudio se justifica en el plano económico porque con el plan de mejora de seguridad de los activos de información que se va a implementar, se van a reducir los riesgos de la seguridad relacionada con la información, se van a evitar pérdidas de información y tiempo, y como consecuencia de ello, se dan evitar costos innecesarios ocasionados por pérdida de información, reparación de activos informáticos, reparación de hardware, asignación de personal especializado a resarcimiento de los daños que pueda causar la exposición a los riesgos en los sistemas informáticos.

Se justifica metodológicamente porque los usuarios del sistema de información del gobierno regional de Ancash van a adquirir las habilidades, capacidades y competencias sobre la aplicación del estándar ISO/IEC 27001, así como de la metodología PDCA de Deming, los cuales van a contribuir en orientar y guiar el desarrollo de las actividades de la planificación, implementación, control y actuación sobre el aseguramiento de la información relacionadas con los procesos operativos y adminsitrativos que desarrollan los colaboradores del Gobierno Regional de Ancash haciendo uso del sistema informático.

El presente estudio es importante porque va a alcanzar un plan de mejora de seguridad estudiada aplicando el estándar internacional ISO/IEC 27001 Con plena aplicación de las fases del ciclo de Deming, su posterior implementación va a proteger los activos de información y la información en su conjunto, sobre todo de información altamente confidencial; este estudio también demuestra relevancia porque va a aportar con la seguridad de la información, cuyos resultados van a favorecer la continuidad la operatividad del sistema de información, así como también va a contribuir en la imagen de la institución en función a la seguridad de sus activos informáticos.

El uso continuo de los sistemas de información ha propiciado Unido a la importancia y el valor que tiene la información que genera cualquier institución, han generado que estos activos estén siempre en riesgo de cualquier tipo de ataque, estos son los problemas que sufren todas aquellas instituciones que utilizan un determinado sistema de información, Teniendo en cuenta estos problemas, a nivel internacional, las instituciones gubernamentales, así como las empresas Privadas del mundo han adoptado una cierta cantidad de técnicas y métodos para poder enfrentar las inseguridades a los que se exponen sus sistemas de información. Las técnicas adaptadas consisten en la aplicación de estándares internacionales, tales como el ISO 27001, metodologías que se han desarrollado para tal fin, tales como Magerit, mejora continua, ISO 27002, etc. (Dussan, 2006). Todos estos estándares contribuyen con guía y orientación, así como también mejores prácticas en el uso

de las tecnologías de información con la finalidad de garantizar la seguridad de los activos informáticos, en ese sentido, las instituciones están obligadas a adoptar esos estándares para que puedan reducir los riesgos de exposición de sus activos informáticos (Alexander, 2007).

A nivel nacional, el Gobierno de Perú está constituido por 24 regiones o departamentos, cada región tiene un sistema de información relativamente complejo, dentro de ella, los usuarios generan diversos tipos de información en función al valor, importancia y confidencialidad. No toda la información tiene la misma importancia, pero se generan archivos con importancia que tienen alto valor, estos archivos deben ser resguardados con la máxima seguridad para que los interesados ajenos. no puedan acceder a ella y variar las dimensiones de la información relacionados con la accesibilidad, integridad y confidencialidad. Todos los gobiernos regionales a nivel nacional han registrado ataques internos y externos, sobre todo en los archivos relacionados con la ejecución de obras públicas, también estas instituciones y videncia que sus sistemas están expuestos a diversos tipos de riesgos, los cuales deben ser atendidos con la finalidad de reducir los problemas relacionados con la seguridad objeto de estudio (Baldeon, 2021).

Los archivos de mayor importancia y confidenciales se generan generalmente en las unidades o áreas de Gerencia Regional de Desarrollo Económico, Gerencia Regional de Desarrollo Social, Gerencia regional Planeamiento, Presupuesto y Acondicionamiento Territorial, Gerencia Regional de Infraestructura, etc., En ese sentido, los postulantes a la ejecución de este tipo de obras pueden vulnerar la confidencialidad de los archivos con la finalidad de obtener ventajas en el momento de la asignación de los proyectos de construcción pública; es por ello que varias regiones del país han adoptado diversos tipos de mecanismos y técnicas para reducir la exposición a riesgos de sus activos informáticos.

A nivel local, el Gobierno Regional de Ancash, dispone de un sistema informático basado en red, la cual utiliza para generar los diversos archivos y

activos de información con diversos niveles de valor, en esta institución gubernamental se observa que existen Riesgos de seguridad de la información en cada una de sus áreas, debido a que escasamente están aplicando estándares de seguridad de información, la gestión de riesgos que están aplicando no es muy adecuado para el nivel de tecnología y la generación de cantidad de información que generan, sobre todo en los archivos de alta confidencialidad que se generan en las gerencias ya indicadas anteriormente. También se observan problemas de falta de guía y orientación en el uso de los sistemas de información relacionados con la seguridad de la información. Estas deficiencias están generando demoras y costos en cada una de las áreas, situación que la administración del Gobierno Regional debe solucionar en el corto plazo.

De no resolverse los problemas encontrados En el corto plazo, la situación de la seguridad podría ir deteriorándose conforme pasa el tiempo, lo cual podría generar un aumento de costos y retrasos para la institución, es por ello que, con la presente investigación se plantea realizar un plan de mejora de seguridad de la información, aplicándole estándares ISO/IEC 27001 Con la finalidad de identificar los activos informáticos que se encuentran en riesgo, así como también, poder alcanzar la guía y orientación basado en el estándar indicado relacionado con la gestión de riesgos a los que podrían exponerse cada uno de los elementos del sistema de información de esta institución gubernamental.

Ante esta realidad problemática, se plantea formular el problema sobre ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash? Como problemas específicos se ha considerado: ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Ancash? ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Económico del Gobierno Regional de Ancash? ¿En qué

medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Social del Gobierno Regional de Ancash? ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Infraestructura del Gobierno Regional de Ancash?

Con el propósito de alcanzar el objetivo de la investiagación, se desea conocer la influencia de la aplicación del Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash en donde se establezcan las actividades la investigacion, en funcion a ello, se conceptualizan y operacionalizan las variables en estudio.

Plan de mejora de seguridad de la información: Es un documento institucional en donde se plasman las normas, estándares, controles y políticas que deben ser socializados a los trabajadores para su cumplimiento, tienen como objetivo garantizar la seguridad de la información mediante la protección de los activos informáticos de un sistema de información en un nivel mejorado aceptable, los activos informáticos en función a la capacidad de protección desarrollada por la administración (Mora, 2020).

Activos informáticos: Se denomina activo informático al conjunto de software, hardware, instalaciones, información, recursos de conectividad, todos estos elementos forman parte del sistema de información de una determinada empresa, estos activos informáticos son utilizados en el desarrollo de los procesos de gestión de índole administrativo y operativos de la empresa, el resultados es la generación y tratamiento de la información, activo muy valorado, es por ello, la necesidad de se les debe garantizar su seguridad (Tupia, 2010).

Dimensiones de la Seguridad de la Información. en el estudio se tomaron las dimensiones de **Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial.** dimensión que tiene como indicadores al

Hardware, software, nube, redes sociales. Estos indicadores son los que contienen los riesgos que se generan con su uso por parte de los usuarios. **Gerencia Regional de Desarrollo Económico.** esta dimensión contiene a los siguientes indicadores: Identificación de riesgos, Identificación de vulnerabilidades, Conocimiento de ataques, y Nivel de protección. **Gerencia Regional de Desarrollo Social. Gerencia Regional de Infraestructura**

(Zapata, 2020).

Tabla 1

Operacionalizacion de la variable

Variable	Dimensiones	Ítems
Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001	Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial	¿Con que frecuencia se reportan robos, ataques informáticos de cualquier tipo en el sistema de información en las Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?

		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?
	Gerencia Regional de Desarrollo Económico	¿Con que frecuencia se reportan robos, ataques informáticos de cualquier tipo en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Económico?
		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Desarrollo Económico?
	Gerencia Regional de Desarrollo Social	¿Con que frecuencia se reportan robos, ataques informáticos de cualquier tipo en el sistema de información en la Gerencia Regional de Desarrollo Social?
		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Desarrollo Social?
		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Desarrollo Social?
		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Desarrollo Económico?

		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Desarrollo Social?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Social?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Social?
		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Desarrollo Social?
	Gerencia Regional de Infraestructura	¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Infraestructura?
		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Infraestructura?

En la investigación se plantea como hipótesis: El Plan de mejora aplicando el estándar ISO/IEC 27001 influye positivamente en la seguridad de la información en el Gobierno Regional de Ancash.

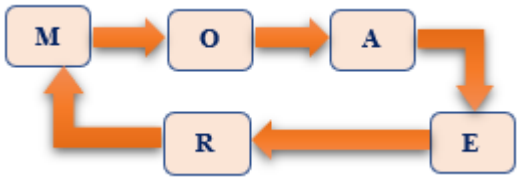
Asimismo, se formuló el objetivo general: Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash. Así mismo. Los objetivos específicos:

- Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Ancash.
- Establecer en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Económico del Gobierno Regional de Ancash.
- Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Social del Gobierno Regional de Ancash.
- Establecer en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Infraestructura del Gobierno Regional de Ancash.

II. METODOLOGÍA

El tipo de estudio fue no experimental debido a que no se tuvo que manipular la variable plan de mejora de la seguridad de la información con la finalidad de medir efectos positivos o negativos en la seguridad indicada. El tipo de investigación en función a la captación de datos fue transversal lo cual significó la realización una sola observación o medición en todo el proceso investigativo. El enfoque que se tuvo que aplicar fue positivista, también conocido como cuantitativo, ya que se trabajó con datos de indicadores de tipo numérico. (Hernández et al, 2019).

El diseño de la presente investigación fue descriptivo porque se tuvo que describir la influencia del plan de mejora en la seguridad de la información, se describió la aplicación del estándar ISO/IEC 27001, se describió estadística descriptiva, y se tuvieron que describir los resultados (Hernández et al, 2019). El esquema de diseño de la presente investigación fue:



Donde:

M = Constituido por los usuarios del sistema de la institución objeto de estudio

O = Observación del uso y normas

A = Análisis del sistema y de la norma internacional ISO/IEC 27001

E = Evaluación o medición de los datos e información

R = Resultados

Población: estuvo conformada por del sistema de información del Gobierno Regional de Ancash, la misma que estuvo constituida por 123 usuarios del sistema de información de esta institución gubernamental que fue utilizada para el desarrollo de los procesos operativos y adminsitrativos en cada unidad, en la siguiente tabla se indican las unidades y la cantidad de los usuarios.

Tabla 2

Población de usuarios del sistema de información del Gobierno Regional

N°	Unidad o área	Cantidad de usuarios
01	Gerencia Regional de Planeamiento Presupuesto y Acondicionamiento Territorial	07
02	Gerencia Regional de Desarrollo Económico	08
03	Gerencia Regional de Desarrollo Social	06
04	Gerencia Regional de Infraestructura	07
05	Gerencia General Regional	06
06	Gerencia Regional de Administración	06
07	Gerencia Regional de Recursos Naturales y Gestión del Medio Ambiente	06
	TOTAL	**46**

Fuente: Elaboracion propia

Muestra: La muestra estuvo estructurada por el mismo tamaño de la población, esto es, 29 usuarios del sistema de información de la Región Ancash.

Tabla 3

Muestra de usuarios del sistema de información del Gobierno Regional

N°	Unidad o área	Cantidad de usuarios
01	Gerencia Regional de Planeamiento Presupuesto y Acondicionamiento Territorial	07
02	Gerencia Regional de Desarrollo	08

	Económico	
03	Gerencia Regional de Desarrollo Social	06
04	Gerencia Regional de Infraestructura	07
	TOTAL	**29**

Técnica: Como técnica aplicó la observación, análisis de los estados situacionales de los activos informáticos del sistema de información relacionados con la seguridad de los archivos y documentos generados dentro del Gobierno Regional de Ancash, y encuesta; los datos se obtuvieron de las cuatro unidades o áreas más importantes de esta institución gubernamental, se tuvo en cuenta la aplicación del estándar ISO/IEC 27001.

Instrumento: El instrumento que se aplicó fue el cuestionario, en este instrumento, los encuestados tuvieron que llenar los datos teniendo en cuenta a las preguntas trazadas relacionados con la seguridad de la información en función a la aplicación del estándar objeto de estudio.

Debido a que el instrumento tuvo que ser creado por el investigador y deba ser aplicado sin ningún tipo de impedimentos como parte del proceso investigativos, se tuvo que determinar la confiabilidad de este instrumento mediante la aplicación del método de Alfa de Cronbach, el instrumento fue aplicado debido a que el valor de Alfa de Cronbach fue mayor a 0.80. También se tuvo que determinar la validez del instrumento aplicando el método de Juicio de Expertos, para este caso, se alcanzó a cada experto el instrumento y las hojas de validación para que puedan realizar el proceso de validación; el instrumento validado fue aceptado para su respectiva aplicación en el presente estudio porque el promedio de las calificaciones del instrumento fue muy bueno o excelente.

Tabla 4

Técnicas e instrumentos de investigación

Técnicas	**Instrumentos**
Observación, analisis y encuesta	Cuestionario

Análisis documental	Textos, tesis, artículos científicos, revistas cientificas e investigaciones antecedentes

Fuente: Elaboracion propia

La metodología en el desarrollo del presente estudio que tuvo como finalidad desarrollar un plan de mejora de seguridad de la información fundamentada en la norma internacional ISO/IEC 27001, se aplicó la metodología denominada Ciclo de Deming o ciclo PHVA, la misma que comprende las siguientes fases o etapas:

Planificar, en esta fase se tuvo que planificar con alcance integral la implementación del sistema de gestión de la seguridad de los activos de informáticos, esto consistió en planificar la seguridad de la información en todas las áreas del Gobierno Regional de Ancash. Se establecieron los objetivos de seguridad para cada área, se desarrolló el análisis de los riesgos en función a las funciones y generación de información confidencial, importante y de valor institucional considerable, se analizaron los riesgos, vulnerabilidades y peligros a los que pudieron estar expuestos el servidor, computadoras clientes, se identificaron las actividades y se organizaron en función del personal que los tuvo que realizar, se establecieron las políticas, procesos y conjunto de actividades que contribuyeron en el aseguramiento de la seguridad informática.

Implementar: Esta fase comprendió el desarrollo de la implementación del plan de seguridad, esta fase se inició con el desarrollo de acciones preventivas con la finalidad de evitar eventos o situaciones de riesgos que pudieron dañar los servidores, computadoras clientes, periféricos, activos informáticos, etc., en esta fase se buscó proteger al sistema de información y a la información en su conjunto desde la perspectiva física y lógica, lo cual significó que se debieron proteger los activos físicos y la parte de programación, información digital y software. La fase de implementación implicó que en cada área de la organización se debieron detectar los riesgos de cada activo de información y ejecutar los procesos de detección, registrarlos, resolver los problemas de riesgos, así como, dar respuesta a los

accidentes e incidentes de seguridad en relación a los procesos, política, controles y procedimientos del sistema de seguridad de la información.

Fase de control o de verificación: Después de realizado la etapa anterior, es decir, la fase de ejecución, siempre fue necesario controlar las actividades y procesos realizados, estos procesos consistieron en verificar si los riesgos han sido bien identificados, si los procesos de reducir los riesgos han sido mejorados de acuerdo a lo planificado, se desarrolló el monitoreo de cada una de las áreas trabajadas, se auditó y se controló el sistema y control de todas las unidades o elementos que conformaron el Sistema de información. La técnica de control se pudo realizar mediante la observación, el análisis y aplicación de auditorías internas y externas. La fase de verificación implicó desarrollar procesos y actividades de evaluación y comparación de cómo se estuvo realizando la implantación del sistema de seguridad de la información comparado con los objetivos y políticas establecidas, implicó evaluación del control de las actividades realizadas, finalmente, esta fase terminó con el alcance de un informe en donde se detallaron las actividades buenas y deficientes realizadas, así como también, las sugerencias respecto a lo auditado.

Actuación, mantenimiento y mejora: La fase de actuar consistió en que las autoridades correspondientes debieron propiciar el tratamiento de mejora a las actividades o procesos que fueron considerados como que no tuvieron satisfacción en las políticas y normas establecidas con los procesos que no estuvieron cumpliendo con garantizar un adecuado control de la seguridad de la información, implicó actuar sobre los riesgos que mantuvieron sus niveles como tal, consistió en actuar en los factores que pusieron en peligro la seguridad de información, así como también, desarrollar las acciones correctivas, esta fase también implicó informar sobre los resultados encontrados y las acciones que se realizaron para poder mejorar las irregularidades encontradas. Esta fase se fundamentó en los resultados obtenidos en una auditoría o evaluación interna, esto significó que se tuvo que mejorar las

deficiencias que habían sido detectadas mediante un proceso oficial de evaluación o auditoría.

III. RESULTADOS

Objetivo específico 1

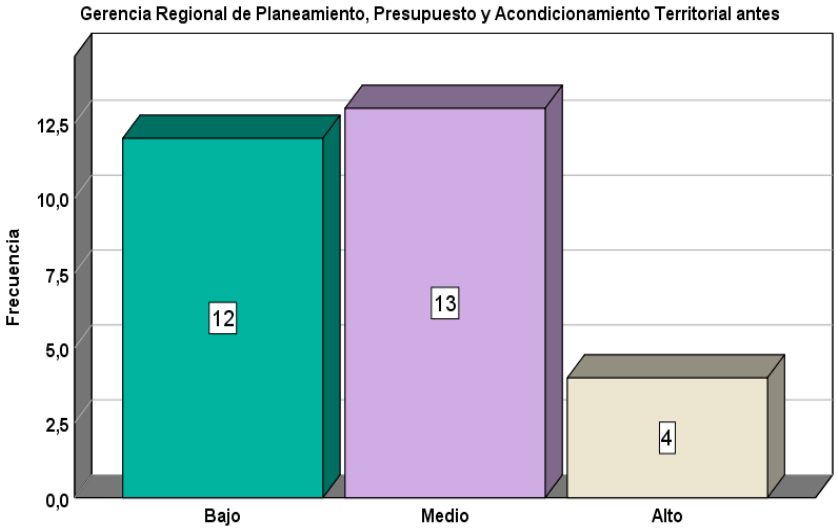
Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Ancash.

Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial antes

Tabla 5
Frecuencia Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial antes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	12	41,4	41,4	41,4
	Medio	13	44,8	44,8	86,2
	Alto	4	13,8	13,8	100,0
	Total	29	100,0	100,0	

Figura 1
Frecuencia Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial antes



Se encontró en el antes que en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial 12 usuarios (41.4%) del sistema de información indicaron que la seguridad de la información fue bajo, 13 encuestados (44.8%) señalaron que fue medio y, 4 encuestados (13.8%) señalaron que la seguridad de la información fue alta.

Tabla 6
Media y varianza de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial antes

y1=mi	f1	y1f1	y21	y21f1
1	12	12.0	1.0	12.0
2	13	26.0	4.0	52.0
3	4	12.0	9.0	36.0
Sumas	**29**	**50.0**	**14.0**	**100.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{50.0}{29} = 1.72$$

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{100.0 - \frac{(50.0)^2}{29}}{28}} = 0.7019$$

La media fue 1.72, lo cual indicó estuvo que el nivel de seguridad de la información antes fue bajo con varianza de 0.7019.

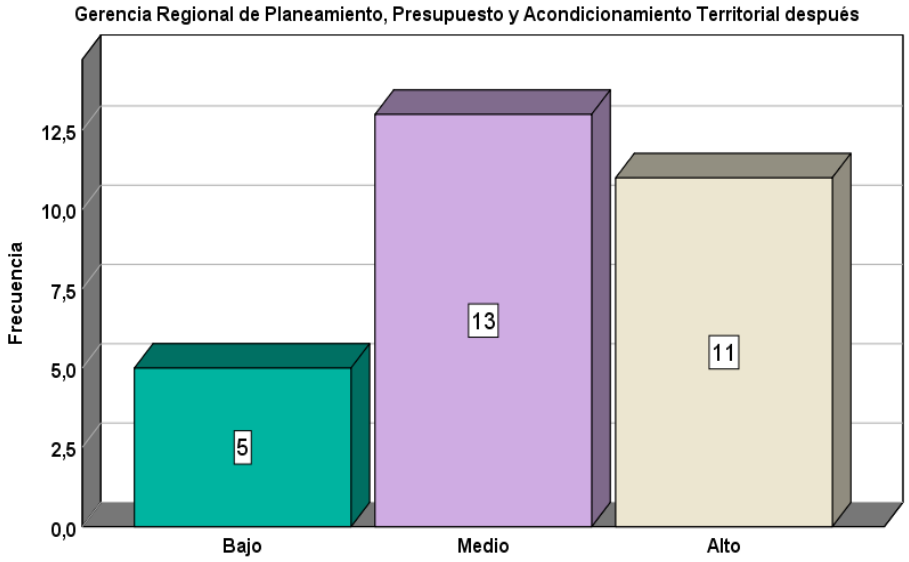
Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial después

Tabla 7
Frecuencia Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial después

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	5	17,2	17,2	17,2
	Medio	13	44,8	44,8	62,1
	Alto	11	37,9	37,9	100,0
	Total	29	100,0	100,0	

Figura 1

Frecuencia Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial después



Se encontró en el después que en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial 5 usuarios (17.2%) del sistema de información indicaron que la seguridad de la información fue bajo, 13 encuestados (44.8%) señalaron que fue medio y, 11 encuestados (37.9%) señalaron que la seguridad de la información fue alta.

Tabla 8

Media y varianza de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial después

y1=mi	f1	y1f1	y21	y21f1
1	5	5.0	1.0	5.0
2	13	26.0	4.0	52.0
3	11	33.0	9.0	99.0
Sumas	**29**	**64**	**14**	**156**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{64.0}{29} = 2.21$$

Cálculo de la varianza

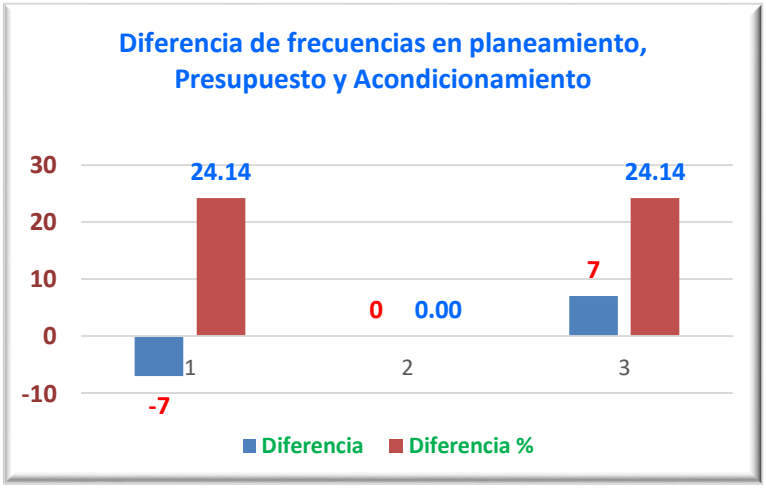
$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{156.0 - \frac{(64.0)^2}{29}}{28}} = 0.7260$$

La media fue 2.21, lo cual indicó estuvo que el nivel de seguridad de la información antes subió a media con varianza de 0.7019.

Tabla 9
Diferencia de frecuencias de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial

y1=mi	f1	f1	Diferencia	Diferencia %
1	12	5	-7	24.14
2	13	13	0	0.00
3	4	11	7	24.14
Sumas	**29**	**29**		

Figura 2
Diferencia de frecuencias de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial



La diferencia de las frecuencias entre el antes y después en el nivel bajo fue -7 lo cual indicó que según el 24.14% de los encuestados la seguridad de la información pasó de bajo a alto; la frecuencia en el nivel medio no se incrementó, mientras que, en el nivel alto, la diferencia fue 7, esto indicó que el 24.14% pasó de media alta. La diferencia porcentual fue calculada por d = 0.48*100/1.72 = 28.00%

Tabla 10
Diferencia de medias de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial

Media antes	Media después	Diferencia	Diferencia %
1.72	2.21	0.48	28.00

La diferencia media de las frecuencias antes y después en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial fue 0.48, esto significó que la media tuvo influencia en la mejora de la seguridad de la información en un 28.00%

Objetivo específico 2

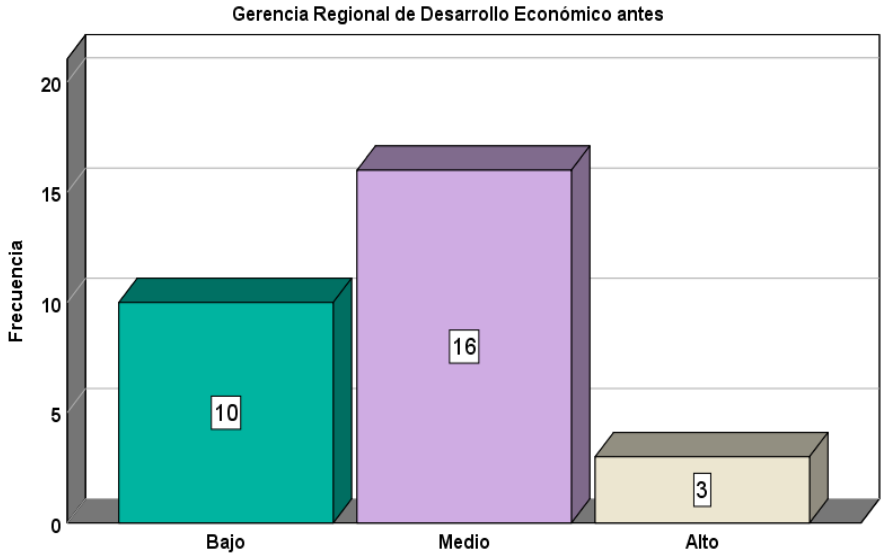
Establecer en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Económico del Gobierno Regional de Ancash.

Gerencia Regional de Desarrollo Económico antes

Tabla 11
Frecuencia de Gerencia Regional de Desarrollo Económico antes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	10	34,5	34,5	34,5
	Medio	16	55,2	55,2	89,7
	Alto	3	10,3	10,3	100,0
	Total	29	100,0	100,0	

Figura 3
Frecuencia de Gerencia Regional de Desarrollo Económico antes



Se encontró que en la seguridad de la información en la Gerencia Regional de Desarrollo Económico 10 usuarios del sistema de información (34.5%) indicaron que la seguridad de la información fue bajo, 16 encuestados (55.2%) señalaron que fue medio y, 3 encuestados señalaron que la seguridad de la información fue alta.

Tabla 12
Media y varianza de la Gerencia Regional de Desarrollo Económico antes

y1=mi	f1	y1f1	y21	y21f1
1	10	10.0	1.0	10.0
2	16	32.0	4.0	64.0
3	3	9.0	9.0	27.0
Sumas	**29**	**51.0**	**14.0**	**101.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{51.0}{29} = 1.76$$

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{101.0 - \frac{(51.0)^2}{29}}{28}} = 0.6356$$

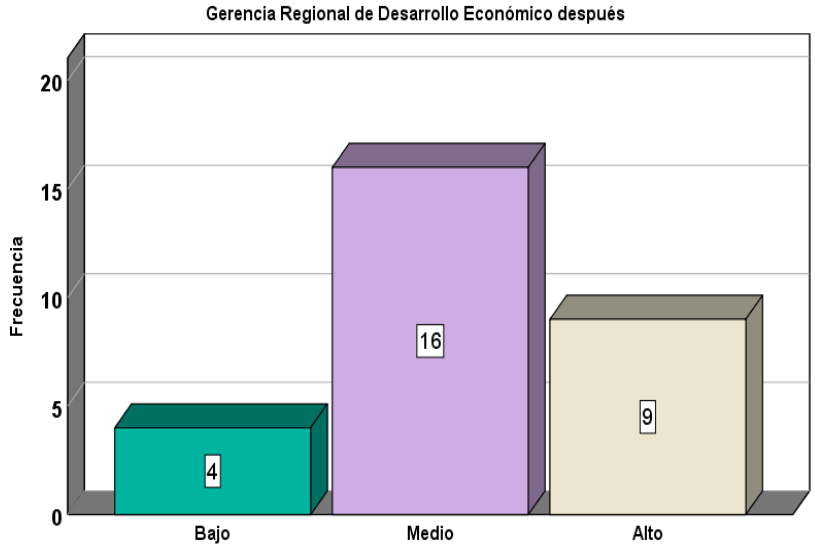
La media fue 1.76, lo cual indicó que el nivel de seguridad de la información antes fue bajo con varianza de 0.6356.

Gerencia Regional de Desarrollo Económico después

Tabla 13
Frecuencia Gerencia Regional de Desarrollo Económico después

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	4	13,8	13,8	13,8
	Medio	16	55,2	55,2	69,0
	Alto	9	31,0	31,0	100,0
	Total	29	100,0	100,0	

Tabla 4
Frecuencia Gerencia Regional de Desarrollo Económico después



Se encontró en el después que, en la seguridad de la información en la Gerencia Regional de Desarrollo Económico, 4 usuarios (13.8%) del sistema de información indicaron que la seguridad de la información fue bajo, 16 encuestados (55.2%) señalaron que fue medio y, 9 encuestados (31.0%) señalaron que la seguridad de la información fue alta.

Tabla 14
Media y varianza de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial después

y1=mi	f1	y1f1	y21	y21f1
1	4	4.0	1.0	4.0
2	16	32.0	4.0	64.0
3	9	27.0	9.0	81.0
Sumas	**29**	**63.0**	**14.0**	**149.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{63}{29} = 2.17$$

Cálculo de la varianza

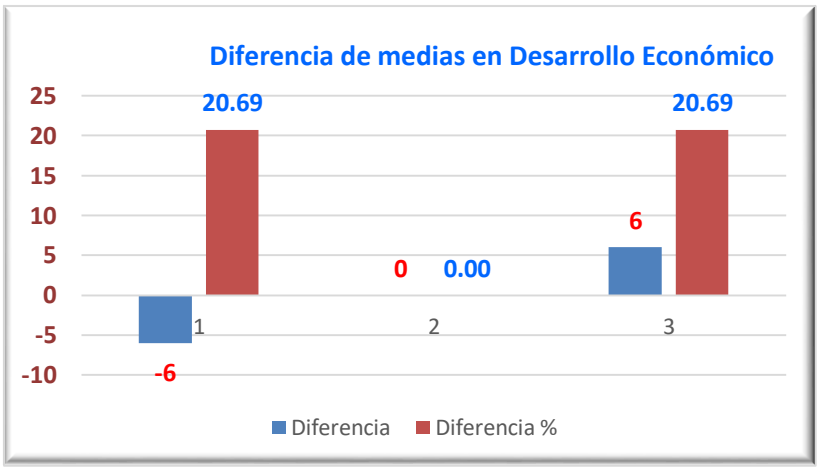
$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{149.0 - \frac{(63.0)^2}{29}}{28}} = 0.63584$$

La media fue 2.17, lo cual indicó estuvo que el nivel de seguridad de la información antes subió a media con varianza de 0.7636.

Tabla 15
Diferencia de frecuencias de la Gerencia Regional de Desarrollo económico

y1=mi	f1	f2	Diferencia	Diferencia %
1	10	4	-6	20.69
2	16	16	0	0.00
3	3	9	6	20.69
Sumas	**29**	**29**	**29**	

Figura 5
Diferencia de frecuencias de la Gerencia Regional de Desarrollo económico



La diferencia de las frecuencias entre el antes y después en el nivel bajo fue -6 lo cual indicó que según el 20.69% de los encuestados la seguridad de la información pasó de bajo a medio; la frecuencia en el nivel medio no se incrementó, mientras que, en el nivel alto, la diferencia fue 6, esto indicó que el 20.69% pasó de media alta.

Tabla 16
Diferencia de medias de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial

Media antes	Media después	Diferencia	Diferencia %
1.76	2.17	0.41	23.53

La diferencia media de las frecuencias antes y después en la Gerencia Regional de Desarrollo Económico fue 0.41, esto significó que la media tuvo influencia en la mejora de la seguridad de la información en un 23.53%

Objetivo específico 3

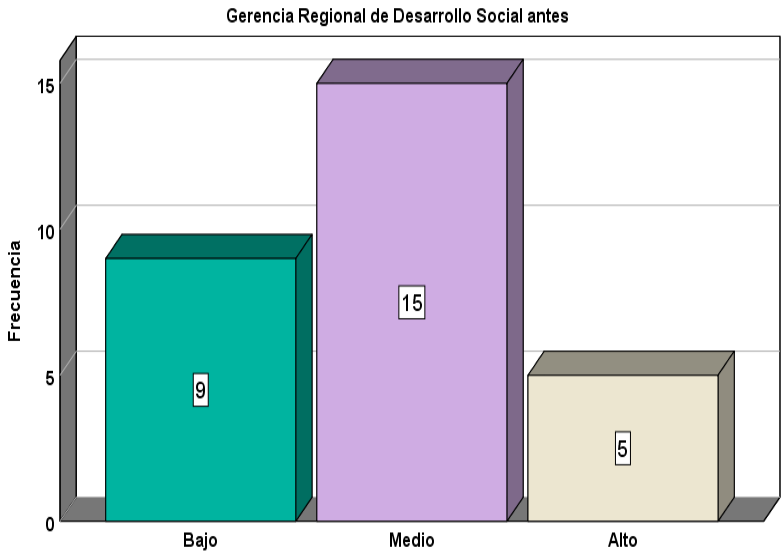
Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Social del Gobierno Regional de Ancash.

Gerencia Regional de Desarrollo Social antes

Tabla 17
Frecuencia Gerencia Regional de Desarrollo Social antes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	9	31,0	31,0	31,0
	Medio	15	51,7	51,7	82,8
	Alto	5	17,2	17,2	100,0
	Total	29	100,0	100,0	

Figura 6
Frecuencia Gerencia Regional de Desarrollo Social antes



Se encontró que en la seguridad de la información en la Gerencia Regional de Desarrollo Social 9 usuarios (31.0%) del sistema de información indicaron que la seguridad de la información fue bajo, 15 encuestados (51.7%) señalaron que fue

medio y, 5 encuestados (17.2%) señalaron que la seguridad de la información fue alta.

Tabla 18
Media y varianza de la Gerencia Regional de Desarrollo Social antes

y1=mi	f1	y1f1	y21	y21f1
1	9	9.0	1.0	9.0
2	15	30.0	4.0	60.0
3	5	15.0	9.0	45.0
Sumas	**29**	**54.0**	**14.0**	**114.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{54}{29} = 1.86$$

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{114.0 - \frac{(54.0)^2}{29}}{28}} = 0.6930$$

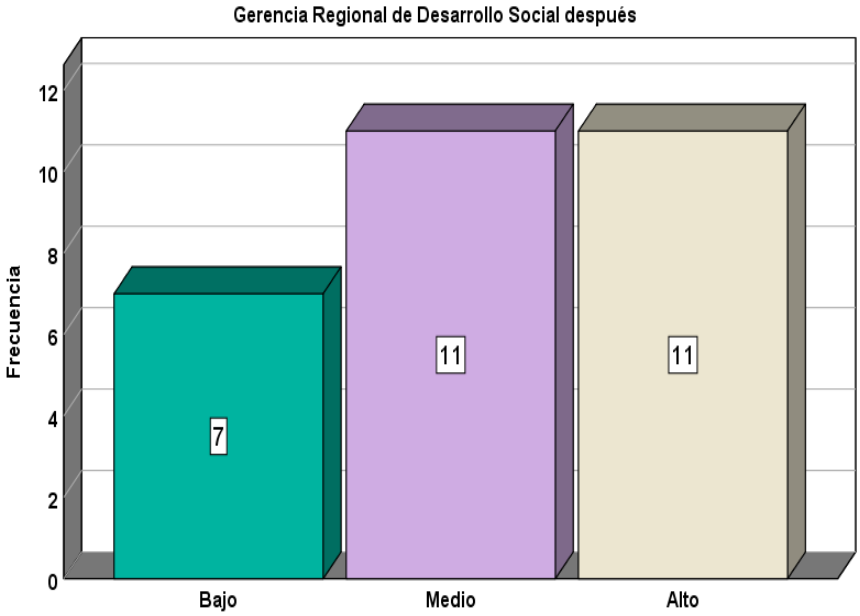
La media fue 1.86, lo cual indicó estuvo que el nivel de seguridad de la información antes fue bajo con varianza de 0.6930.

Gerencia Regional de Desarrollo Social después

Tabla 19
Frecuencia Gerencia Regional de Desarrollo Social

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	7	24,1	24,1	24,1
	Medio	11	37,9	37,9	62,1
	Alto	11	37,9	37,9	100,0
	Total	29	100,0	100,0	

Figura 7
Frecuencia Gerencia Regional de Desarrollo Social



Se encontró en el después que en la seguridad de la información en la Gerencia Regional de Desarrollo Social 7 usuarios (24.1%) del sistema de información indicaron que la seguridad de la información fue bajo, 11 encuestados (37.9%) señalaron que fue medio y, 11 encuestados (37.9%) señalaron que la seguridad de la información fue alta.

Tabla 20
Media y varianza de la Gerencia Regional de Desarrollo Social después

y1=mi	f1	y1f1	y21	y21f1
1	7	7.0	1.0	7.0
2	11	22.0	4.0	44.0
3	11	33.0	9.0	99.0
Sumas	**29**	**62.0**	**14.0**	**150.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{62}{29} = 2.14$$

Cálculo de la varianza

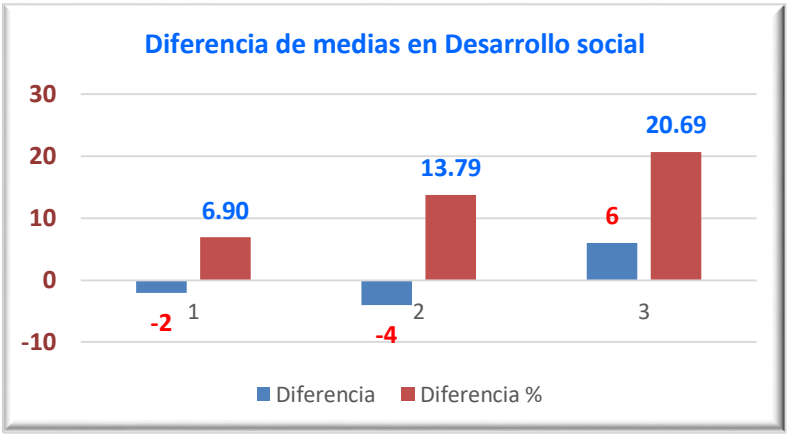
$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{150.0 - \frac{(62.0)^2}{29}}{28}} = 0.7894$$

La media fue 2.14, lo cual indicó estuvo que el nivel de seguridad de la información antes subió a media con varianza de 0.7894

Tabla 21
Diferencia de frecuencias de la Gerencia Regional de Desarrollo Social

y1=mi	f1	f1	Diferencia	Diferencia %
1	9	7	-2	6.90
2	15	11	-4	13.79
3	5	11	6	20.69
Sumas	**29**	**29**		

Tabla 8
Diferencia de frecuencias de la Gerencia Regional de Desarrollo Social



La diferencia de las frecuencias entre el antes y después en el nivel bajo fue -2 lo cual indicó que según el 6.90% de los encuestados la seguridad de la información pasó de bajo a medio; en el nivel medio fue -4 lo cual indicó que según el 13.79% de los encuestados la seguridad de la información pasó de medio a alto, mientras que, en el nivel alto, la diferencia fue 6, esto indicó que para el 20.69% pasó de media alta.

Tabla 22
Diferencia de medias de la Gerencia Regional de Desarrollo Social

Media antes	Media después	Diferencia	Diferencia %
1.86	2.14	0.28	14.81

La diferencia media de las frecuencias antes y después en la Gerencia Regional de Desarrollo Social fue 0.28, esto significó que el plan de mejora de la seguridad de la información tuvo influencia en la mejora de la seguridad de la información en un 14.81%

Objetivo específico 4

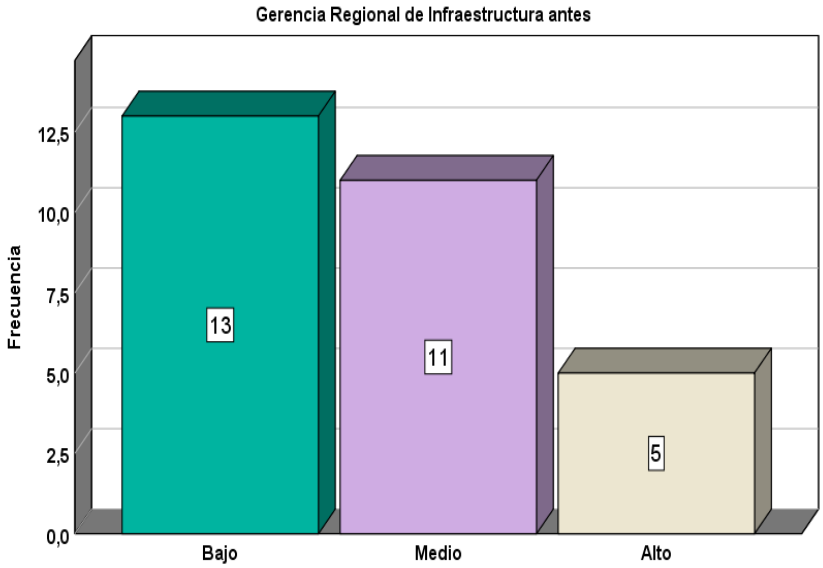
Establecer en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Infraestructura del Gobierno Regional de Ancash.

Gerencia Regional de Infraestructura antes

Tabla 23
Frecuencia Gerencia Regional de Infraestructura antes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	13	44,8	44,8	44,8
	Medio	11	37,9	37,9	82,8
	Alto	5	17,2	17,2	100,0
	Total	29	100,0	100,0	

Figura 9
Frecuencia Gerencia Regional de Infraestructura antes



Se encontró que en la seguridad de la información en la Gerencia Regional de Infraestructura 13 usuarios (44.8%) del sistema de información indicaron que la seguridad de la información fue bajo, 11 encuestados (37.9%) señalaron que fue medio y, 5 encuestados (17.2%) señalaron que la seguridad de la información fue alta.

Tabla 24
Media y varianza de la Gerencia Regional de Infraestructura antes

y1=mi	f1	y1f1	y21	y21f1
1	13	13.0	1.0	13.0
2	11	22.0	4.0	44.0
3	5	15.0	9.0	45.0
Sumas	**29**	**50.0**	**14.0**	**102.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{50.0}{29} = 1.72$$

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{102.0 - \frac{(50.0)^2}{29}}{28}} = 0.7510$$

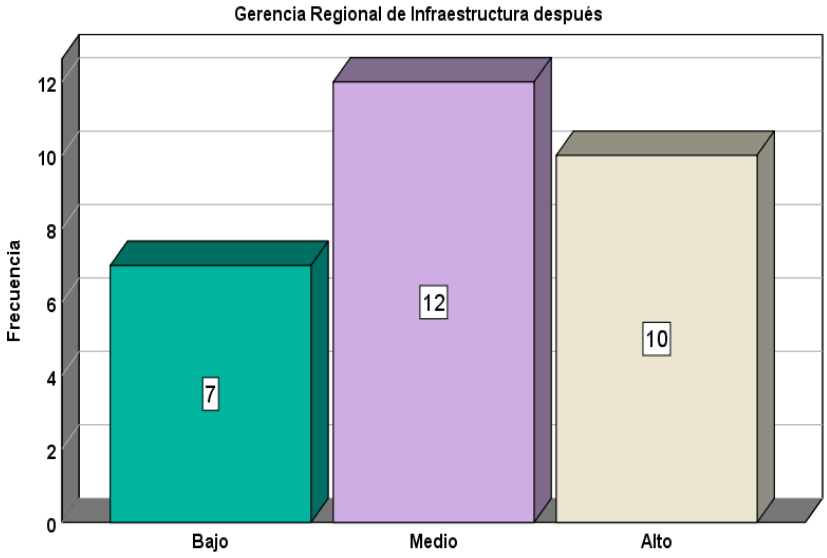
La media fue 1.72, lo cual indicó que el nivel de seguridad de la información antes fue bajo con varianza de 0.7510.

Gerencia Regional de Infraestructura después

Tabla 25
Frecuencia Gerencia Regional de Infraestructura después

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	7	24,1	24,1	24,1
	Medio	12	41,4	41,4	65,5
	Alto	10	34,5	34,5	100,0
	Total	29	100,0	100,0	

Figura 10
Frecuencia Gerencia Regional de Infraestructura después



Se encontró en el después que en la seguridad de la información en la Gerencia Regional de Infraestructura 7 usuarios (24.1%) del sistema de información indicaron que la seguridad de la información fue bajo, 12 encuestados (41.4%) señalaron que fue medio y, 10 encuestados (34.5%) señalaron que la seguridad de la información fue alta.

Tabla 26
Media y varianza de la Gerencia Regional de Infraestructura después

y1=mi	f1	y1f1	y21	y21f1
1	7	7.0	1.0	7.0
2	12	24.0	4.0	48.0
3	10	30.0	9.0	90.0
Sumas	**29**	**61.0**	**14.0**	**145.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{61.0}{29} = 2.10$$

Cálculo de la varianza

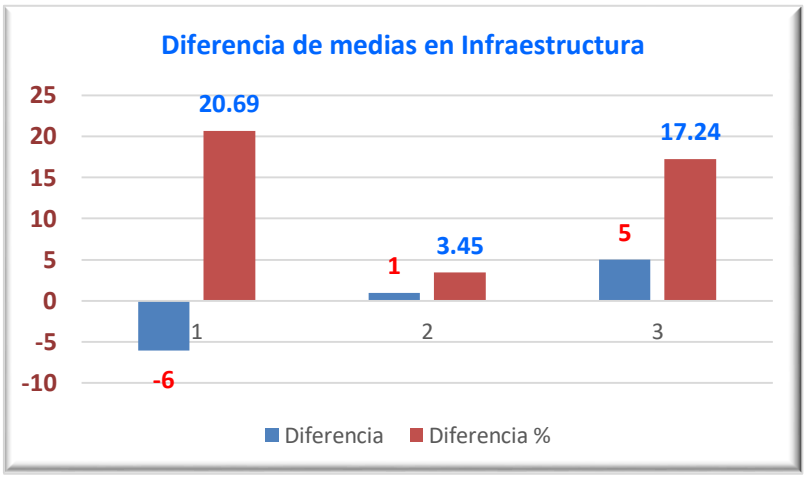
$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{145.0 - \frac{(61.0)^2}{29}}{28}} = 0.75720$$

La media fue 2.10, lo cual indicó que el nivel de seguridad de la información después subió a media con varianza de 0.7572.

Tabla 27
Diferencia de frecuencias de la Gerencia Regional de Infraestructura después

y1=mi	f1	f1	Diferencia	Diferencia %
1	13	7	-6	20.69
2	11	12	1	3.45
3	5	10	5	17.24
Sumas	**29**	**29**		

Figura 11
Diferencia de frecuencias de la Gerencia Regional de Infraestructura después



La diferencia de las frecuencias entre el antes y después en el nivel bajo fue -6 lo cual indicó que según el 20.69% de los encuestados la seguridad de la información pasó de bajo a medio; en el nivel medio fue 1 lo cual indicó que según el 3.45% de los encuestados la seguridad de la información pasó de medio a alto, mientras que, en el nivel alto, la diferencia fue 5, esto indicó que para el 17.24% pasó de media alta.

Tabla 28
Diferencia de medias de la Gerencia Regional de Infraestructura

Media antes	Media después	Diferencia	Diferencia %
1.72	2.10	0.38	22.00

La diferencia media de las frecuencias antes y después en la Gerencia Regional de Infraestructura fue 0.38, esto significó que el Plan de mejora tuvo influencia en la mejora de la seguridad de la información en un 22.0%

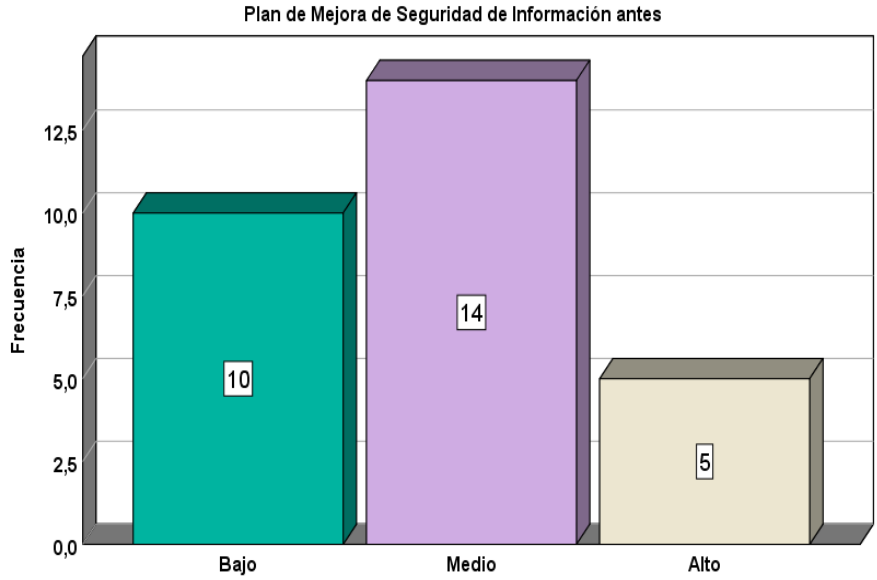
Objetivo general

Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash.

Tabla 29
Frecuencia Plan de mejora aplicando estandar ISO/IEC 27001 antes

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	10	34,5	34,5	34,5
	Medio	14	48,3	48,3	82,8
	Alto	5	17,2	17,2	100,0
	Total	29	100,0	100,0	

Figura 12
Frecuencia Plan de mejora aplicando estandar ISO/IEC 27001 antes



Se encontró que antes de aplicar el Plan de mejora con estandar ISO/IEC 27001 antes 10 usuarios (34.5%) del sistema de información indicaron que la seguridad de

la información fue bajo, 14 encuestados (48.3%) señalaron que fue medio y, 5 encuestados (17.2%) señalaron que la seguridad de la información fue alta.

Tabla 30
Media y varianza de la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial antes

y1=mi	f1	y1f1	y21	y21f1
1	13	13.0	1.0	13.0
2	11	22.0	4.0	44.0
3	5	15.0	9.0	45.0
Sumas	**29**	**50.0**	**14.0**	**102.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{53.0}{29} = 1.83$$

Cálculo de la varianza

$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{111.0 - \frac{(53.0)^2}{29}}{28}} = 0.7106$$

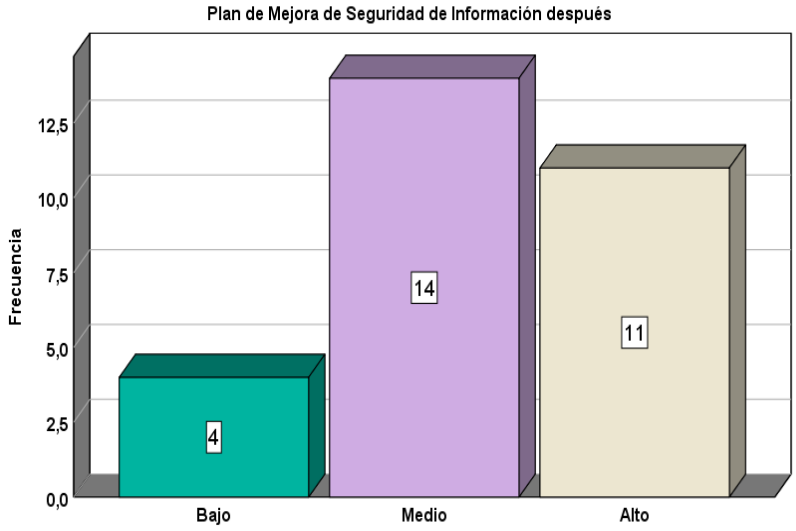
La media fue 1.83, lo cual indicó estuvo que el nivel de seguridad de la información antes fue bajo con varianza de 0.7106

Plan de Mejora de Seguridad de Información después

Tabla 31
Frecuencia de Pland e mejora de la seguridad de la información después

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Bajo	4	13,8	13,8	13,8
	Medio	14	48,3	48,3	62,1
	Alto	11	37,9	37,9	100,0
	Total	29	100,0	100,0	

Figura 13
Frecuencia de Pland e mejora de la seguridad de la información después



Se encontró que antes de aplicar el Plan de mejora con estándar ISO/IEC 27001 después 4 usuarios (13.8%) del sistema de información indicaron que la seguridad de la información fue bajo, 14 encuestados (48.3%) señalaron que fue medio y, 11 encuestados (37.9%) señalaron que la seguridad de la información fue alta.

Tabla 32
Media y varianza de Plan de mejora de la seguridad de informaciónl después

y1=mi	f1	y1f1	y21	y21f1
1	4	4.0	1.0	4.0
2	14	28.0	4.0	56.0
3	11	33.0	9.0	99.0
Sumas	**29**	**65.0**	**14.0**	**159.0**

Cálculo de la media

$$\bar{x}_1 = \frac{\sum y_1 f_1}{n} = \frac{65.0}{29} = 2.24$$

Cálculo de la varianza

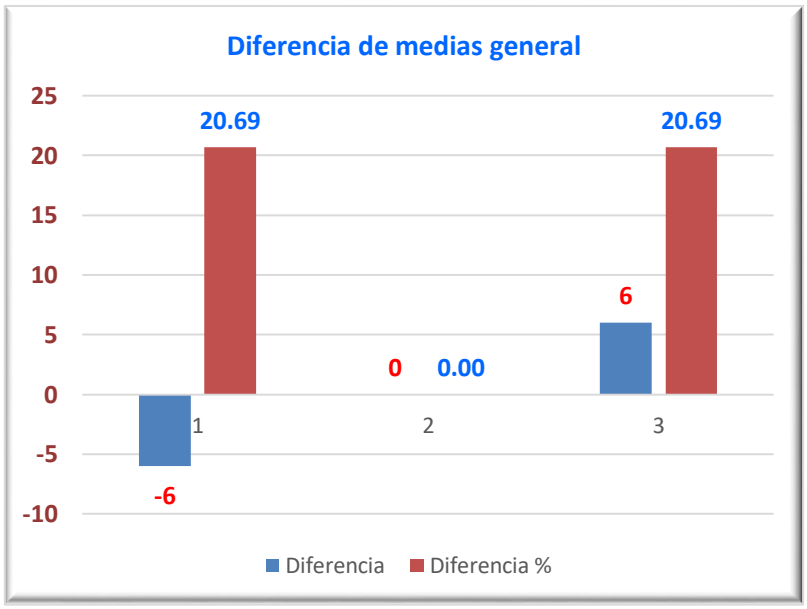
$$S_1^2 = \sqrt{\frac{\sum y_1^2 f_1 - \frac{(\sum y_1 f_1)^2}{n}}{n-1}} = \sqrt{\frac{159.0 - \frac{(65.0)^2}{29}}{28}} = 0.6895$$

La media fue 2.24, lo cual indicó que el nivel de seguridad de la información antes subió a media con varianza de 0.6895

Tabla 33
Diferencia de frecuencias de Plan de mejora de la seguridad de la información

y1=mi	f1	f1	Diferencia	Diferencia %
1	10	4	-6	20.69
2	14	14	0	0.00
3	5	11	6	20.69
Sumas	**29**	**29**		

Figura 14
Diferencia de frecuencias dePlan de mejora de la seguridad de la información



La diferencia de las frecuencias entre el antes y después en el nivel bajo fue -6 lo cual indicó que según el 20.69% de los encuestados la seguridad de la información pasó de bajo a medio; la frecuencia en el nivel medio no se incrementó, mientras que, en el nivel alto, la diferencia fue 6, esto indicó que el 20.69% pasó de media alta.

Tabla 34

Resumen de diferencia de medias de frecuencias dePlan de mejora de la seguridad de la información

O. Específicos	media antes	Media después	Diferencia	Diferencia %
1	1.72	2.21	0.48	28.00
2	1.76	2.17	0.41	23.53
3	1.86	2.14	0.28	14.81
4	1.72	2.10	0.38	22.00
Promedio	**1.77**	**2.16**	**0.39**	**22.09**

El Plan de mejora aplicando el estándar ISO/IEC 27001 influyó en un 22.09% en la seguridad de la información en el Gobierno Regional de Ancash**.**

IV. ANÁLISIS Y DISCUSIÓN

En este estudio se encontró que el Plan de mejora aplicando el estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en las instalaciones de la Región Ancash, este resultado contrasta significativamente con lo encontrado por Baldeón (2021) quién indicó que el 94% de los usuarios necesitaban mejorar la seguridad de la información del sistema de información, el 26% indicaron que existió plan de contingencia, el 74% indicaron que no existió el pan de contingencia. Respecto a las conclusiones en la investigación antecedentes se indicó que la implantación de ISO/IEC 27001:2013 favoreció la reducción de los egresos económicos y mejoró la funcionalidad de los procesos internos, lo cual coincide en parte con los resultados del presente estudio.

En el actual estudio se tuvo como resultado que el Plan de mejora aplicando el estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en el objeto de estudio, este resultado concuerda con lo encontrado por Mendoza (2019) en el sentido de que fue urgente el requerimiento de la implantación de un Sistema que pueda gestionar aspectos relacionados con la Seguridad de la información para la institución, coincide también en la condiciones iniciales de inseguridad encontrados, ya que en la investigación antecedente se encontró 637 amenazas con impactos calificados como moderado, alto y muy alto.

Se tuvo como resultado en esta investigación que el Plan de mejora aplicando el estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en el espacio estudiado ancashino, este resultado coincide parcialmente con lo encontrado por Alban (2018) concluyó que el plan informático fue desarrollado en función a las necesidades operativas y administrativas de la sociedad, y que contribuyó en mejorar la seguridad de los procesos llevados a cabo de manera adecuada, sistematizada y correcta con los controles y las responsabilidades del cuidado de los activos más importantes como la información de cualquier ataque interno y externo, riesgo y vulnerabilidades. Concluyó que estándar internacional utilizado permitió perfeccionar la seguridad de la información como se requería.

En este estudio se tuvo como resultado que el Plan de mejora utilizando el estándar internacional ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en las instalaciones del objeto estudiado, este resultado concuerda muy ligeramente con lo encontrado por Simbaña (2018) en donde se encontró que el espacio estudiado no tuvo un área específica de informática, que se tuvo que organizar los documentos en calidad de regulatorios para que brinden una normativa y responsabilidades, que se tuvo que garantizar a que los usuarios sean ubicados o asignados por sus actividades. Se tuvo que establecer políticas y normas de seguridad con fines de perfeccionar la seguridad en función a activos de información y los medios computacionales. El plan de contingencia ayudó en la determinación de riesgos relacionados con la infraestructura tecnológica, para ello propuso el plan preventivo. Coincide parcialemnte en que el plan informático 2018-2022 cimentado en el estándar normativo internacional utilizado va a optimizar la seguridad de los activos de la información, instalaciones tecnológicas en el objeto estudiado.

En esta investigación se tuvo como resultado que el Plan de mejora aplicando el estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en el espacio analizado, este resultado coincide significativamente con lo encontrado por Abanto (2023) quien encontró que se estaba aplicando la norma con un 0% del cumplimiento de la norma indicada, en función a ello, tuvieron que elabora un modelo de gestión de seguridad informática fundamentado en función a lo estipulado en la norma indicada donde se ejecutó la gestión de riesgo con todos los controles implicados controles. Determinaron a los activos que tuvieron relación con la seguridad en las dimensiones lógica y física del objeto estudiado. Evaluaron la amenaza, vulnerabilidad y los riesgos a los que estaban expuestos todos los activos, específicamente los de tecnología informática bajo la norma indicadas y aplicadas. Concluyeron que la propuesta del modelo de seguridad basado en la norma aplicada se pudo evidenciar métodos de mejora de la seguridad de la información en un 23.6%.

En este estudio se tuvo el resultado en que el Plan de mejora con uso del estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de los activos de información en el Gobierno Regional de Ancash, este resultado coincide ligeramente con lo encontrado por García (2020) en donde se encontró que el 91.00% indicaron que no se estaba brindando seguridad y que el 9.00% señalaron que si se brindaba seguridad de la información. El 87% presentó conocimientos adecuados en la aplicación de la norma ISO 27001, mientras que el 13% no presentaron esos conocimientos, el 96% indicó que, si demostraron un cierto nivel de cultura en el cumplimiento de los protocolos de seguridad indicada, y el 4% indicaron que no lo realzaban. Concluyó que se evaluó el estado situacional de cada uno de los procesos de seguridad en función al estándar internacional estudiado, debido a ello, se pudo establecer los problemas de seguridad de la información. Que los marcos de referencia contribuyeron en realizar la propuesta de mejoras en la seguridad. Concluyó se realizó la propuesta de la aplicación de la Norma aplicada con la finalidad de mejorar la seguridad en el espacio estudiado.

Se tuvo como resultado en esta investigación que el Plan de mejora aplicando el estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en el Gobierno Regional de Ancash, este resultado tuvo coincidencia significativas con lo encontrado por Poma (2019) quien concluyó que existió necesidad de realizar la propuesta de la elaboracion del plan de mejora de la seguridad de la información fundamentada en la norma internacional estudiada y aplicada en la investigación. Que la elaboración del Plan de Seguridad aportó de manera muy significativa en el procesos de perfeccionamiento de la seguridad de la información, esta mejorar consistió en lograr un perfeccionamiento de la dimensión confidencialidad en 17.59%, respecto a la dimensión disponibilidad fue 30.51% y en la dimensión integridad fue 14.66%. Que la propuesta va a aportar para la institución con la emisión de sugerencias con la finalidad de darle la importancia debida a los procesos y tareas que se debieron realizar y considerar durante la etapa de analisis y evaluación adecuada del Sistema de Control Interno, así como en las actualizaciones futuras.

En el presente estudio se tuvo que el Plan de mejora aplicando el estándar ISO/IEC 27001 influyó positivamente en un 22.09% en la seguridad de la información en el espacio estudiado, este resultado coicide parcialmente con lo encontrado por Guardia (2020) encontró que las necesidades sobre seguridad en el antes fue 83% y después 95%, los trabajadores que conocen la política seguridad fueron 0.05% y 1005, los que cumplieron con la seguridad fueron 1% y 90%, las vulnerabilidades fueron 40% y 90%, los riesgos altos fueron 0% 0% y 38%. Concluyó que el modelo de seguridad de la información permitió el logro de minimizar los riesgos de seguridad de la información, logró optimizar riesgos de los activos admitiendo conocer que equipos de TI estaban disponibles y operativos. Respecto a las conclusiones ambas investigaciones coinciden en que el personal fue crítico en el proceso de sensibilización respecto a la seguridad informática, con el modelo, el personal fue consciente que la información fue muy importante en los aspectos de seguridad, que las amenazas estuvieron presentes generando vulnerabilidad con riesgos probables de afectar a la seguridad del información del sistema informático.

.

V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Se concluyó a nivel general que la diferencia de las frecuencias entre el antes y después de la aplicación del pan de mejora en el nivel bajo fue -6 lo cual indicó que según el 20.69% de los encuestados la seguridad de la información pasó de bajo a medio; la frecuencia en el nivel medio no se incrementó, mientras que, en el nivel alto, la diferencia fue 6, esto indicó que el 20.69% pasó de media alta. El Plan de mejora aplicando el estándar ISO/IEC 27001 influyó en un 22.09% en la seguridad de la información en el Gobierno Regional de Ancash.

La aplicación del pan de mejora en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial en el antes y después en el nivel bajo fue -7 lo cual indicó que según el 24.14% de los encuestados la seguridad de la información pasó de bajo a medio; la frecuencia en el nivel medio no se incrementó, mientras que, en el nivel alto, la diferencia fue 7, esto indicó que el 24.14% pasó de media alta. La diferencia media de las frecuencias antes y después fue 0.48, esto significó que la media tuvo influencia en la mejora de la seguridad de la información en un 28.00%

La aplicación del plan de mejora en la gerencia Regional de Desarrollo Económico generó diferencia de las frecuencias entre el antes y después en el nivel bajo fue -6 lo cual indicó que según el 20.69% de los encuestados la seguridad de la información pasó de bajo a medio; la frecuencia en el nivel medio no se incrementó, mientras que, en el nivel alto, la diferencia fue 6, esto indicó que el 20.69% pasó de media alta. La diferencia media de las frecuencias antes y después fue 0.41, esto significó que la media tuvo influencia en la mejora de la seguridad de la información en un 23.53%

La aplicación del plan de mejora generó en la Gerencia Regional de Desarrollo Social diferencia de las frecuencias entre el antes y después en el nivel bajo fue -2 lo cual indicó que según el 6.90% de los encuestados la seguridad de la información pasó de bajo a medio; en el nivel medio fue -4 lo cual indicó que según el 13.79% de los encuestados la seguridad de la información pasó de medio a alto, mientras que, en el nivel alto, la diferencia fue 6, esto indicó que para el 20.69% pasó de media alta. La diferencia media de las frecuencias antes y después fue 0.28, esto significó

que el plan de mejora de la seguridad de la información tuvo influencia en la mejora de la seguridad de la información en un 14.81%

La aplicación del plan de mejora generó en la Gerencia Regional de Infraestructura La diferencia de las frecuencias entre el antes y después en el nivel bajo fue -6 lo cual indicó que según el 20.69% de los encuestados la seguridad de la información pasó de bajo a medio; en el nivel medio fue 1 lo cual indicó que según el 3.45% de los encuestados la seguridad de la información pasó de medio a alto, mientras que, en el nivel alto, la diferencia fue 5, esto indicó que para el 20.69% pasó de media alta. La diferencia media de las frecuencias antes y después fue 0.38, esto significó que el Plan de mejora tuvo influencia en la mejora de la seguridad de la información en un 22.00%

.

VI. RECOMENDACIONES

Las Gerencias Regionales del Gobierno Regional de Ancash deben tomar decisiones oportunas sobre la seguridad de la información en función a los resultados encontrados en el presente estudio, las decisiones deben partir con la preparación y capacitación adecuada de los usuarios del sistema de información en cada gerencia regional, pero con la participación consciente y decidida de las gerencias y los usuarios del sistema de información.

La Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial tiene que continuar con la capacitación a los empleados de su área en los aspectos de la seguridad de información, así como en el conocimiento de la aplicación del plan de mejora basado en el estándar ISO/IEC 27001, para ello debe contactar con las demás gerencias regionales y contratar a expertos en el tema y que hayan trabajado con gobiernos regionales dentro del país.

La Gerencia Regional de Desarrollo Económico debe continuar con la capacitación a los empleados de su área en los aspectos de la seguridad de información, así como en el conocimiento de la aplicación del plan de mejora basado en el estándar ISO/IEC 27001, debe generar conciencias en los usuarios del sistema de información debido a que es un área en donde se genera información sensible y de alta importancia para esta organización gubernamental. La gerencia debe monitorear mensualmente el manejo de la seguridad de información en su área, específicamente en temas relacionados a ataques internos y externos.

La Gerencia Regional de Desarrollo Social, según los resultados obtenidos, debe seguir con la capacitación de los usuarios informáticos de su área en los temas de la seguridad de información, debe asegurarse que los usuarios conozcan los aspectos teóricos del estándar ISO/IEC 27001 y su aplicación en la generación de seguridad a los archivos y software en general, para ello debe capacitarlos adecuadamente con profesionales adecuados, las

capacitaciones deben ser trimestralmente con evaluaciones de los resultados en función de la inversión realizada.

La Gerencia Regional de Infraestructura debe controlar de forma contínua y sostenida los indicadores de la seguridad de la información de su gerencia, para ello debe capacitar a los empleados que usen el sistema de información en la generación de información importante, debe asegurarse que cada usuario tenga el conocimiento de la aplicación del plan de mejora basado en el estándar ISO/IEC 27001, puede hacer uso de recursos motivacionales para mejorar la seguridad de la información en su gerencia.

VII. AGRADECIMIENTOS

A Dios por permitirme el objetivo de ser profesional, al Gobierno Regional de Ancash por el espacio, los datos e información alcanzada, a la Universidad San Pedro por todo el apoyo recibido a través sus docentes quienes supieron darme la formación y enseñanza, a todos mis compañeros quienes contribuyeron en el logro de mi objetivo, ser profesional.

Jackson

VIII. REFERENCIAS BIBLIOGRÁFICAS

Abanto, Cesar Daniel y Rivera, José Ángel (2023). *Propuesta de un modelo de sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la Sede central del gobierno regional de Huánuco – 2022.* [Tesis de grado]. Universidad nacional Hermilio Valdizán. Huánuco Perú.

AENOR (2014). *Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información*. ISO/IEC 27001:2013. Madrid: AENOR

Alban, Wilson Alejandro (2018). *Plan informático 2018-2022 basado en la norma ISO/IEC 27001-2013 para mejorar la seguridad de la información y recursos tecnológicos en la empresa "Consulting Group" Santo Domingo*. [Tesis de grado]. Universidad Regional Autónoma de Los Andes. Ecuador.

Alexander, A. G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información* (1era. ed.). Bogotá: Alfaomega Colombiana S.A.

Alvarado, F. J. (2016). *La Gestión de la Seguridad de la Información en el Régimen Peruano de Protección de Datos Personales.* Lima. Recuperado el 14 de diciembre de 2018, de www.gobiernodigital.gob.pe/docs/Política_Nacional_de_Ciberseguridad.pdf

Baca, G. (2016). *Introducción a la Seguridad Informática*. México: Grupo Editorial Patria, S.A. de C.V.

Baldeón, Andrés Fabián (2021). *Plan informático basado en la norma ISO/IEC v27001:2013 para mejorar la calidad en los procesos de la seguridad de la información y recursos tecnológicos de la unidad educativa particular*

Nazaret en la ciudad de Santo Domingo. [Tesis de grado]. Universidad Regional Autónoma de los Andes. Ecuador.

Berrio, J. P. (2016). *Metodologia para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001* [Tesis de Maestría]. Medellín, Colombia.

Borja, Y. A. (2018). Plan *de Seguridad Informática* Espe. Sangolqui.

Calder, A. (2009). *Implementando Seguridad de la Información basado en ISO 27001/27001 A Management Guide.* Van Haren Publishing. Recuperado el 23 de setiembre de 2019.

Chicano, E. (2014). *Gestión de incidentes de seguridad informática*. Málaga: IC Editorial.

Chicano, E. (2015). *Gestión de Incidentes de Seguridad Informática*. Primera edición ed. Málaga: Editorial I, editor; 2015.

Costas Santos, J. (2014). *Seguridad Informática*. Madrid: RA-MA.

Dussan, C. A. (2006). *Políticas de seguridad informática*. Vol 2., núm. 1 enero junio, 2006, pp. Colombia.

García, Rodolfo Augusto (2020). *Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020*. [Tesis de grado]. Universidad Católica Los Ángeles de Chimbote. Piura Perú.

Gómez, L. & Fernández, P. (2015). *Cómo implantar un SGSI según UNE-ISO/IEC 27001:2014 y su aplicación en el Esquema Nacional de Seguridad*. Primera edición. Madrid, España: AENOR.

Guardia, Rómulo Víctor (2020). *Diseño de un modelo de seguridad de la información para minimizar los riesgos informáticos en la gestión académica del Instituto de Educación Superior Tecnológico Público "Eleazar Guzmán Barrón"-Huaraz" – 2018*. [Tesis de maestría]. Universidad Nacional Santiago Antúnez de Mayolo. Huaraz Perú.

Hamid, N. (2007). *Information Security and Ethics: Concepts, Methodologies, Tools, and Applications: Concepts, Methodologies, Tools, and Applications*. Estados Unidos: IGI Global.

Hernández, R., Fernández, C., & Baptista, L. (2019). *Metodología de la Investigación*. Valencia: Sexta Edición. México.

INCIBE. (20 de 08 de 2019). *Guía sobre borrado seguro de la información*. España.

ISACA, (2009) *Risk IT- Marco de Riesgos de TI.* España-Madrid.

ISO/IEC. (2016). *Information technology-Security Techniques-Information security management systems-overview and vocabulary*. Switzerland: ISO.

ISO2700.es. (2012). *Sistema de gestión de la seguridad de la información*. Madrid.

Llontop, G. C. (2018). *Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks* [Tesis de Maestría]. Lima.

Mendoza, Denís Celín (2019). *Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la Secretaría de Educación Departamental del Norte de Santander*. [Tesis de grado]. Universidad Nacional Abierta y a Distancia. Colombia.

Mercado, J. E. (2016). *Modelo de gestión de seguridad de la información para el E-Gobierno* [Tesis de Maestría]. Lima.

Migga, K. J. (2020). *Guide to Computer Network Security.* Chattanooga: Springer.

Miguel, C. (2015). *Protección de datos y seguridad de la información*. Cuarta ed. España: Ra-Ma.

Mohamed, E. (2019). *Cybersecurity and Secure Information Systems: Challenges and Solutions in Smart Environments*. Cairo: Springer.

Mora, J. (2020). *El Sistema de Gestión de Seguridad de la Información bajo la norma NTE ISO/IEC 27001 en Instituciones de Educación Superior en Ecuador*. ROCA, Vol 16(1), Págs 546-559 ISSN: 2074-0735. RNPS: 2090. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=741435

Poma, Luis Alejandro (2019*). Plan de mejora de la seguridad de la información del Seguro Social de salud – EsSalud aplicando estándar ISO/IEC 27001*. [Tesis de grado]. Universidad Privada Antenor Orrego. Trujillo Perú.

PORTANTIER. (2013). *Seguridad Informática*: Aprenda como implementar soluciones desde la visión del experto.

Rodríguez, J. M., & Peralta, I. (2019). *Gestión de riesgo Margerit*. Obtenido de www.tithimk.com.

Romero, M. I., Figueroa, G. L., Vera, D. S., Álava, J. E., Parrales, G. R., Álava, C. J., ., Castillo, M. A. (2018). *Introducción a la seguridad informática y al análisis de vulnerabilidades.* Alicante: Ciencias.

Samaniego, E. A. y Ponce J. A. (2021). *Fundamentos de seguridad informática. Universidad Estatal de Quevedo*. Ecuador: Compas. ISBN:978-9942-33-426-8

Simbaña, Maria Karina (2028). *Plan informático 2018-2022 basado en la norma ISO/IEC 27001:2013 para mejorar la seguridad de la información, infraestructura y recursos tecnológicos en la unidad educativa fiscal "Kasama" de Santo Domingo*. [Tesis de grado]. Universidad Regional Autónoma de Los Andes. Ecuador.

Smith, R. E. (2019). *Elementary Information Security*. Estados unidos: Jones & Bartlett Learning.

Tupia, M. F. (2010). *Administración de la Seguridad de Información*. Callao: Tupia Consultores y Auditores S.A.C.

Vidalina, F. N. (2012). *Sistema de Gestión de Seguridad de la Información*. Primera ed. Venezuela: EAE.

ANEXOS Y APÉNDICES

Anexo 01:

Matriz de Consistencia

Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023

PROBLEMA DE INVESTIGACIÓN	OBJETIVOS	HIPÓTESIS	METODOLOGÍA
Problema General ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash? **Problemas específicos** ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Ancash? ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Económico del Gobierno Regional de Ancash? ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Social del Gobierno Regional de Ancash? ¿En qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Infraestructura del Gobierno Regional de Ancash?	**Objetivo General** Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en el Gobierno Regional de Ancash. **Objetivos Específicos** Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial del Gobierno Regional de Ancash. Establecer en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Económico del Gobierno Regional de Ancash. Determinar en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de Desarrollo Social del Gobierno Regional de Ancash. Establecer en qué medida el Plan de mejora aplicando el estándar ISO/IEC 27001 influye en la seguridad de la información en la Gerencia Regional de	**Hipótesis General** El Plan de mejora aplicando el estándar ISO/IEC 27001 influye positivamente en la seguridad de la información en el Gobierno Regional de Ancash.	Se considera que la investigación es de tipo no experimental. **Diseño de la Investigación** **Diseño:** Descriptivo **Enfoque:** Cuantitativo **Población** Estará conformado por 123 usuarios del sistema de información del Gobierno Regional de Ancash. **Muestra:** Estará conformado por 29 usuarios del sistema de información del Gobierno Regional de Ancash . **Instrumentos de investigación** Ficha de registro de datos

	Infraestructura del Gobierno Regional de Ancash.		

Anexo 02

UNIVERSIDAD SAN PEDRO

ENCUESTA

Bach. Gonzales Torres Jackson Junior

Estimado encuestado: Sírvase responder con absoluta sinceridad la siguiente encuesta que corresponde al estudio del Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023. Sírvase responder la encuesta con responsabilidad y honestidad. Este proceso es totalmente anónimo, se reitera el pedido de absoluta honestidad en sus respuestas. Muchas Gracias por su participación.

FICHA DE REGISTRO DE DATOS

N°	DIM	CUESTIONARIO	ESCALA		
			1	2	3
Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001					
01	Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial	¿Con que frecuencia se reportan robos, ataques informáticos de cualquier tipo en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
02		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
03		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
04		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
05		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
06		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
07		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			

08		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial?			
09	Gerencia Regional de Desarrollo Económico	¿Con que frecuencia se reportan robos, ataques informáticos de cualquier tipo en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
10		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
11		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
12		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
13		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
14		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
15		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
16		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
17	Gerencia Regional de desarrollo social	¿Con que frecuencia se reportan robos, ataques informáticos de cualquier tipo en el sistema de información en la Gerencia Regional de Desarrollo Social?			
18		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Desarrollo Social?			
19		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Desarrollo Social?			
20		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Desarrollo Económico?			
21		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Desarrollo Social?			
22		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Social?			
23		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Desarrollo Social?			
24		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Desarrollo Social?			
25	Gerencia Regional de Infraestructura	¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Infraestructura?			
26		¿Cómo se considera el conocimiento de los roles y responsabilidades de la protección, seguridad en el uso y aplicación en el sistema de información en la Gerencia Regional de Infraestructura?			
27		¿Cómo califica el acceso al uso del sistema informático del personal en su área en el sistema de información en la Gerencia Regional de Infraestructura?			
28		¿Cómo califica la seguridad de la información confidencial en el sistema de información en la Gerencia Regional de Infraestructura?			
29		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Infraestructura?			
30		¿Cómo evalúa la protección de hardware, software e información en el sistema de información en la Gerencia Regional de Infraestructura?			
31		¿Cómo evalúa la existencia de medidas de seguridad de la información en el sistema de información en la Gerencia Regional de Infraestructura?			
32		¿Cómo se considera el conocimiento en seguridad informática del personal en el sistema de información en la Gerencia Regional de Infraestructura?			

LEYENDA

1 Bajo 2 Medio 3 Alto

Anexo 03

Alfa de Cronbach

Nº	PLAN DE MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN APLICANDO ESTÁNDAR ISO/IEC 27001																																				
	Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial								TOT	Gerencia Regional de Desarrollo Económico								TOT	Gerencia Regional de desarrollo social								TOT	Gerencia Regional de Infraestructura								TOT	TOT
	1	2	3	4	5	6	7	8		9	10	11	12	13	14	15	16		17	18	19	20	21	22	23	24		25	26	27	28	29	30	31	32		
1	1	2	2	3	1	3	1	2	1.88	2	3	3	1	2	2	3	1	2.13	1	1	2	2	3	2	3	1	1.88	1	1	2	2	3	1	1	2	1.6	7.5
2	2	1	3	1	1	2	2	1	1.63	3	3	2	2	1	3	1	3	2.25	2	2	1	3	3	3	1	1	2.00	3	2	1	2	1	1	2	1	1.6	7.5
3	2	3	2	3	3	1	2	3	2.38	2	3	1	2	3	2	3	3	2.38	1	2	3	2	3	2	3	3	2.38	3	1	3	3	3	1	2	1	2.1	9.3
4	1	3	3	1	2	1	1	3	1.88	3	1	1	1	3	3	1	2	1.88	1	1	3	3	1	3	1	2	1.88	2	1	1	1	1	3	1	2	1.5	7.1
5	2	1	1	3	2	1	2	1	1.63	1	3	1	2	1	1	3	2	1.75	1	2	1	1	3	1	3	2	1.75	2	1	3	2	3	2	1	3	2.1	7.3
6	2	2	2	2	3	2	2	2	2.13	2	2	2	2	2	3	2	3	2.25	2	2	2	2	2	2	2	3	2.13	3	2	3	3	2	2	2	2	2.4	8.9
7	2	3	2	1	2	1	2	3	2.00	2	1	1	2	3	2	1	2	1.75	1	2	3	2	1	2	1	2	1.75	2	1	2	2	1	3	1	1	1.6	7.1
8	1	1	3	1	2	1	1	1	1.38	3	1	1	1	1	3	1	2	1.63	1	1	1	3	1	3	1	2	1.63	2	1	1	2	1	3	2	1	1.6	6.3
9	3	3	2	2	3	3	3	3	2.75	2	2	3	3	3	2	2	3	2.50	3	3	3	2	2	2	2	3	2.50	3	3	2	3	2	1	1	2	2.1	9.9
10	1	1	2	2	2	2	2	1	1.63	2	2	2	2	1	2	2	2	1.88	2	2	1	2	2	2	2	2	1.88	2	2	2	2	2	1	3	2	2	7.4
Var									0.15									0.08									0.07									0.1	
																																				Suma de varianzas	0.388
																																				Varianza General	1.154
																																				Valor de Alfa	0.885

Validación de instrumento

Anexo 05

Base de datos

Antes

N°	Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001																													
	Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial								Gerencia Regional de Desarrollo Económico								Gerencia Regional de desarrollo social								Gerencia Regional de Infraestructura							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	2	2	2	3	2	2	2	3	1	1	2	2	3	2	1	1	3	2	3	2	3	3	2	3	1	1	1	2	1	1	1
2	2	1	2	1	1	1	1	1	1	2	1	2	1	1	1	2	1	1	3	1	3	1	1	2	1	2	1	2	1	1	1	1
3	3	2	2	2	1	2	2	2	3	2	1	1	2	3	3	1	1	3	2	1	2	1	2	2	3	2	1	1	2	3	3	1
4	1	1	1	1	2	1	1	1	2	1	2	1	1	2	1	1	1	2	1	1	1	2	1	1	2	1	2	1	2	2	1	2
5	2	2	2	2	3	2	2	2	2	2	1	2	1	3	2	1	1	3	2	3	2	3	2	2	2	2	1	2	1	1	1	1
6	2	3	2	3	2	2	2	2	1	1	2	1	2	1	1	1	3	2	2	2	2	2	2	2	1	3	2	1	1	1	1	1
7	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2	1	1	1	3	1	1	1	2	1	2	1	1	1	1	2
8	3	3	3	3	2	3	3	3	3	2	2	1	3	2	3	2	2	3	3	3	3	2	3	2	3	3	2	2	3	2	3	3
9	1	2	2	2	2	2	2	2	2	2	1	2	2	3	1	3	2	2	2	2	2	2	2	2	2	2	1	2	2	3	1	3
10	2	2	1	2	1	1	1	1	1	2	1	1	2	1	2	1	3	1	1	1	1	1	1	1	1	2	1	1	2	1	2	1
11	2	1	3	1	3	3	3	3	3	1	1	2	2	2	2	2	2	2	3	1	2	1	3	2	3	1	1	2	1	1	1	1
12	3	3	2	3	3	3	2	2	2	3	3	3	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3	3	3	3	3
13	2	2	1	2	1	1	1	1	2	1	1	2	2	3	2	1	1	1	1	1	1	1	1	1	2	1	1	2	2	1	1	1
14	3	2	2	2	3	2	2	2	1	2	1	2	1	3	1	3	1	3	2	3	2	3	2	2	1	2	1	2	3	1	1	3
15	2	1	1	2	1	1	1	1	1	2	1	1	2	1	1	1	1	2	1	2	1	2	1	1	1	2	1	1	2	1	1	1
16	2	1	2	1	1	2	1	1	2	2	2	3	2	2	1	2	2	1	2	1	2	1	2	3	2	2	2	3	2	2	2	2
17	3	2	3	3	2	3	3	3	2	2	1	2	3	1	3	2	3	3	3	3	3	3	3	2	3	3	1	3	1	3	3	3
18	1	1	2	1	1	2	1	1	3	3	2	1	2	1	2	1	2	1	2	1	2	1	2	2	3	3	2	1	2	1	2	1
19	2	2	1	1	2	1	2	2	2	1	2	2	1	3	1	3	1	2	1	2	1	1	1	2	2	1	2	2	1	3	1	3
20	2	1	2	3	2	2	1	1	2	2	2	1	3	2	3	2	2	1	2	1	2	2	2	1	2	2	2	1	3	2	3	2
21	3	3	3	2	3	3	3	2	3	3	2	2	2	3	2	3	2	3	3	3	3	3	3	3	3	2	3	3	2	3	3	3
22	1	1	2	1	1	2	1	1	1	2	1	1	2	1	1	1	1	1	2	1	2	1	2	1	1	2	1	2	2	1	1	1
23	1	2	1	2	2	1	2	2	1	1	1	2	2	2	1	1	2	2	1	2	1	1	1	1	1	1	1	2	2	2	1	1
24	1	2	2	1	1	2	1	1	2	2	1	2	2	3	3	2	1	1	2	1	2	1	2	2	2	2	1	2	2	3	3	2
25	1	2	1	2	1	2	1	1	1	2	2	1	2	1	1	1	1	1	2	1	2	1	2	1	1	1	2	1	2	1	1	1
26	1	2	1	1	2	1	1	1	3	3	1	1	3	1	1	3	2	2	1	2	1	2	1	3	3	3	1	1	3	1	1	3
27	2	3	2	2	1	2	2	1	3	2	3	3	3	3	3	3	3	3	3	3	2	3	2	3	3	2	3	3	2	3	3	3
28	1	2	1	1	2	1	2	2	1	1	1	2	1	3	1	1	2	1	2	1	2	2	2	1	1	1	1	2	1	1	1	1
29	3	1	1	3	3	1	3	2	1	1	2	1	3	2	3	3	1	3	1	3	1	3	1	1	1	1	2	1	3	2	3	3

Después

N°	Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001																													
	Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial								Gerencia Regional de Desarrollo Económico antes								Gerencia Regional de desarrollo social antes								Gerencia Regional de Infraestructura							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
1	2	2	3	2	3	2	2	3	3	1	3	2	2	3	1	3	3	3	2	3	3	3	3	3	3	3	2	2	2	3	2	1
2	2	1	2	1	2	1	1	1	2	2	1	2	1	2	1	2	1	1	2	1	3	1	1	1	1	2	1	2	2	1	1	1
3	3	2	2	2	3	2	2	2	3	2	3	2	2	3	3	3	3	3	2	3	3	3	2	3	3	2	3	2	3	3	3	3
4	1	2	2	1	2	1	2	1	2	1	2	2	1	2	1	1	1	2	1	2	2	2	2	2	2	2	2	2	2	2	1	2
5	2	2	2	3	3	2	2	2	2	2	1	2	3	3	2	1	1	3	2	3	2	3	2	2	2	2	1	2	3	2	2	2
6	2	3	2	3	3	2	3	3	3	2	2	3	2	3	3	3	3	2	2	3	3	3	3	2	2	3	2	2	3	2	2	3
7	1	1	1	2	1	1	1	1	2	1	2	1	1	1	1	1	2	1	1	1	3	1	1	1	2	1	2	1	1	1	1	2
8	3	3	3	3	2	3	3	3	3	2	2	2	3	3	3	2	2	3	3	3	3	2	3	3	3	3	3	3	3	2	3	3
9	1	2	2	2	3	2	2	2	2	3	1	2	2	3	2	3	2	2	2	2	2	2	2	2	2	2	3	2	2	3	1	3
10	2	2	1	2	2	2	3	2	1	2	1	3	2	1	2	2	3	1	2	1	2	1	2	1	2	2	1	1	2	1	1	1
11	2	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2	3	3	3	3	2	3	3	2	1	3	3	2	1	1	1	3
12	3	3	2	3	3	3	2	3	3	3	3	3	3	3	3	2	3	2	3	3	3	3	3	3	2	3	3	3	3	3	3	3
13	2	2	3	2	3	3	3	3	2	1	3	2	2	3	2	1	1	2	2	1	3	3	2	1	2	3	3	2	3	3	2	3
14	3	2	2	2	3	2	2	2	1	2	1	2	1	3	1	3	3	1	2	3	2	1	1	3	1	2	3	2	3	3	3	3
15	2	2	1	2	2	2	3	2	3	2	1	2	2	1	2	2	1	2	1	2	1	2	1	1	1	2	1	2	2	2	2	2
16	2	3	2	3	3	2	2	2	2	2	2	3	2	3	1	3	2	3	3	2	2	1	2	2	2	2	2	3	2	2	2	2
17	3	2	3	3	2	3	3	3	2	2	2	3	3	1	3	3	3	3	3	3	3	3	3	2	3	3	2	3	3	3	3	3
18	1	1	2	1	1	2	1	1	3	3	2	3	2	1	2	1	2	1	2	3	2	1	2	2	3	3	2	1	3	1	2	3
19	2	2	1	1	2	1	2	2	2	1	2	2	1	3	1	3	1	2	1	2	1	1	1	2	2	1	2	2	1	3	1	3
20	2	3	2	3	2	3	3	3	2	2	3	3	1	2	3	2	3	3	2	3	2	3	3	3	3	2	3	3	3	3	3	2
21	3	3	3	2	3	3	3	2	3	3	2	2	2	3	2	3	2	3	3	3	3	3	3	3	3	2	3	3	2	3	3	3
22	1	1	2	1	1	2	1	1	1	2	1	1	2	1	1	1	1	1	2	1	2	1	2	1	1	2	1	2	2	1	1	1
23	1	2	1	2	2	1	2	2	2	1	2	2	2	2	3	1	2	2	3	2	1	3	1	3	1	1	1	2	1	2	1	1
24	3	2	2	3	3	3	3	3	2	2	1	2	2	1	1	2	3	3	3	3	2	3	3	2	3	3	3	3	3	3	3	3
25	2	2	1	2	2	2	3	2	1	1	2	1	2	1	1	1	2	1	2	2	2	1	2	2	1	2	2	1	2	2	1	2
26	1	2	3	1	2	1	3	1	3	3	2	2	3	2	3	3	2	2	3	2	1	2	1	3	2	2	1	1	1	1	1	2
27	3	3	2	3	3	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	2	3	2	3	3	2	3	3	2	3	3	3
28	1	2	1	1	2	1	2	1	1	1	1	2	1	3	1	1	2	1	2	1	2	1	1	1	1	1	2	1	1	1	1	1
29	3	2	3	3	3	1	3	2	3	3	2	3	3	2	3	3	3	2	2	3	2	3	3	1	2	3	2	3	3	2	3	3

Anexo 06

Plan de Seguridad de la Información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023

1. Introducción

El presente plan de seguridad de la información con aplicación del estándar ISO/IEC 27001 en el Gobierno Regional de Ancash tiene como finalidad mejorar las condiciones de seguridad de cuatro principales unidades o áreas del Gobierno Regional, estos son, Gerencia Regional de Planeamiento, Presupuesto y Acondicionamiento Territorial, Gerencia Regional de Desarrollo Económico, Gerencia Regional de Desarrollo Social y Gerencia Regional de Infraestructura, para que contribuya en la preservación de la confidencialidad, disponibilidad e integridad de los recursos informáticos.

El Gobierno Regional actualmente tiene el encargo social Planificar el desarrollo integral de la Región Ancash y ejecutar los programas socioeconómicos correspondientes con la finalidad de cumplir con sus funciones operativas y administrativas dispone de diversos tipos y modelos de sistemas informáticos de acuerdo a las necesidades de las diversas unidades o áreas que lo conforman, en el uso de este sistema de información se evidencia la existencia de deficiencias en las políticas de seguridad, específicamente en el uso y tratamiento de la información, en el cuidado de las dimensiones de la información generada, así como en los activos de información, existen carencias en los lineamientos enfocados con la seguridad, considerables deficiencias en el tratamiento de riesgos, los cuales son generados por falta de conocimiento de las vulnerabilidades y amenazas, por otro lado, se observa inconveniente desarrollo de gestión, de actualización de uso de la tecnología, problemas en el conocimiento del uso y tratamiento seguro de hardware y software, escenarios que pueden afectar la seguridad de la información debido a que no se cuenta con un plan o programa que pueda minimizar los peligros o riesgos informáticos que se pudieran presentar.

En este estudio se está considerando el uso de la norma NTP-ISO/IEC 27001 como política para mejorar la seguridad de la información, por lo tanto, la investigación implica que se deba planificar, hacer chequear y actuar; así mismo, el estudio se fundamenta en la norma NTP-ISO/IEC 27001:2014.

2. Situación actual

El Gobierno Regional de Ancash, actualmente dispone de un sistema de información conformado por servidor, impresoras computadoras personales, laptops, sistemas de red, software, usuarios en cada una de las gerencias regionales que utilizan el sistema de información, también dispone de un área de informática que se encarga de dar el soporte a todos los usuarios.

2.1 Archivos de información

El Gobierno Regional de Ancash dispone de un sistema de información basado en red, tienen como elementos al hardware, software, sistema de red y personal que utiliza todo este aparato tecnológico en cada una de las gerencias regionales.

2.2 Las políticas de seguridad

Actualmente, el Gobierno Regional de Ancash dispone de políticas de seguridad de la información bien definidas y claras en el plano teórico, no obstante, presenta bastante falencia en los aspectos de seguridad de la información, en cada gerencia regional se generan diariamente una gran cantidad de información, los cuales deben ser guardados con bastante seguridad, estos archivos son generados por los usuarios de cada gerencia regional, cada usuarios debe cumplir con las normas establecidas respecto a la seguridad de la información que están normadas, el problema que se observa son problemas relacionados con la seguridad de la información, en ese sentido, la actual investigación busca lograr los lineamientos precisos para que cada uno de los colaboradores puedan responder con dominio aceptable sobre la seguridad de la información antes, durante y después del uso del sistema de información.

2.2.1 Política de seguridad física y ambiental

2.2.2 Política de uso de Internet

Todos los empleados del Gobierno Regional de Ancash tienen que utilizar el sistema de información de la organización de forma estricta y de manera específica en el desarrollo de sus funciones laborales operativas o administrativas, queda tajantemente prohibido hacer uso del sistema de la información en otras actividades muy diferentes a los que cada gerencia regional considere pertinente.

2.3 Control de seguridad de la información

2.3.1 Seguridad de los equipos fuera de las instalaciones

El uso de equipo asignado al proceso de datos e información, dentro y fuera del ámbito del Gobierno Regional de Ancash tienen que ser autorizado por el área de informática, para ello debe haber un acuerdo coordinado con anterioridad con esta institución gubernamental. Para lo casos de almacenamiento de datos e información importante o clasificado, necesariamente debe ser aprobado dicha documentación.

2.3.2. Análisis de riesgos

Los problemas de la aparición de riesgos pueden darse en cualquier unidad del Gobierno Regional, estos tipos de riesgos pueden ser:

- Accesos físicos y virtuales de otros usuarios generalmente no autorizado
- Exposición de data e información muy importante y muy confidencial para la unidad y el Gobierno Regional
- Acceso físico o virtual a los sistemas de información y los archivos de personal no autorizado
- Acceso y uso no autorizado de datos e información de una determinada unidad sin el consentimiento de la gerencia o de quienes lo hayan elaborado
- Eliminación, apropiación de registros o archivos de la gerencia regional
- Instalación indebida o no autorizada de software de cualquier tipo, para ello se debe de pedir respectiva autorización
- Acceso de usuarios autorizados del sistema hacia sitios o páginas de internet indebidas o no autorizadas

- Usar el sistema de información del Gobierno Regional para trabajos que no sean propios de una determinada gerencia regional.
- Exponer datos e información confidencial y de alta importancia para la unidad o el Gobierno Regional
- Dañar hardware o software, así como también data e información de manera deliberada
- Realizar cambios a los contenidos de los archivos o registros lógicos y digitales
- Tener claves de sus compañeros de trabajo, en este caso el usuario debes ser amonestado o se le debe aplicar respectiva sanción.

2.3.3. Vulnerabilidades

La vulnerabilidad que presentan mayores frecuencias en un sistema de información en las unidades o gerencias del Gobierno Regional de Ancash son los siguientes:

- Que los usuarios, específicamente de altos cargos, no dispongan de conciencia sobre la importancia de la seguridad de los activos de información, así como, seguridad física y lógica del sistema de información
- Poner contraseñas sencillas o clásicas o de fácil acceso para atacantes internos y externos
- Dar contraseñas o claves a compañeros de trabajo, familiares, amigas o confiar a profesionales de la misma institución gubernamental
- No cambiar contraseñas cada cierto tiempo
- No instalar pertinentemente sistemas antivirus a nivel de hardware y software
- No realizar actualizaciones de forma periódica al sistema antivirus
- No disponer de una política de seguridad, esto es muy importante para institución gubernamental, sobre todo si esas políticas están basadas en normas nacionales e internacionales

- No tener conciencia de seguridad por parte de trabajadores operativos y adminsitrativos
- Bajar archivos indebidos de Internet o de cualquier otra fuente no segura
- Obsolescencia de hardware y software, para ello debe existir una política de actualización de la tecnología TIC
- Mal estado del sistema de cableado o conectividad del sistema de información
- Copia no controlada de la información y datos
- Deficiencias en la gestión del sistema de información
- Insuficiencias en el control de datos de entrada y salida
- Protección física no eficiente o ineficaz

Aplicación de controles

OBJETIVO	CONTROLES	CUMPLIMIENTO	
		SI	NO
Política de Seguridad	Verificar las políticas de seguridad de información del gobierno regional.		
	Existen perfiles profesionales que garanticen la Seguridad de la información del gobierno regional.		
	La gerencia del Gobierno Regional de Ancash está comprometida con la seguridad de la información.		
	Existe coordinación entre la gerencia del gobierno regional y otras áreas en función de mejorar la seguridad de información.		
	Se asignan responsabilidades relacionados con la seguridad de la información.		
	Existen procesos de autorización de cambios de procesamiento de información del gobierno regional.		
	Existen normas de confidencialidad en cada unidad o gerencia.		
	Se hacen revisiones en el uso del sistema de información rutinarias que aseguren la seguridad de la información.		
	Se identifica la existencia de riesgos relacionados con entidades externas		

Gestión de Activos de información	Existe registros de inventarios de activos en cada unidad o gerencia.		
	Se verifican registros de manera periódica, para asegurar el sistema de información en cada unidad o gerencia		
	Se planifica el uso adecuado de hardware y software en cada unidad o gerencia		
	Se clasifican los activos de acuerdo a categorías.		
	Existe técnicas para la atomización del registro de activos.		
Seguridad de los usuarios el sistema de información	Se asignan responsabilidades de los usuarios en cada unidad o gerencia.		
	Existe un proceso de selección para asignar responsables de las copias de seguridad de información.		
	Se realizan verificaciones de términos y condiciones de uso del sistema de información para cada usuario autorizado y no autorizado		
	Existe una gestión de responsabilidades y un encargado de esa gestión		
	Se planifica capacitación y educación en seguridad de la información a cada usuario del sistema de información		
	Existen procedimientos disciplinarios con respecto a la vulnerabilidad de la seguridad de la información.		
	Se registran las incidencias de vulnerabilidad y/o amenazas de la seguridad de la información en cada unidad o gerencia.		
	El personal devuelve los activos que han terminado el contrato o personal en actividad en cada unidad o gerencia		
	Se verifica la eliminación de derechos de acceso al usuario cesado en cada unidad o gerencia.		
Seguridad Física y Ambiental	Existe seguridad física aceptable en cada unidad o gerencia.		
	Existen controles en las entradas de ambientes físico en cada unidad o gerencia.		

	Se verifica la seguridad de oficinas, ambientaciones y medios en cada unidad o gerencia.		
	Existe protección contra riesgos y amenazas externas, respecto a los ambientes.		
	Se comprueba los trabajos en áreas seguras en cada unidad o gerencia.		
	Se comprueban las áreas de acceso público a las instalaciones del sistema de información en cada unidad o gerencia.		
	Se ubican y protegen los elementos del sistema de información en cada unidad o gerencia.		
	Las computadoras se encuentran en un nivel de temperatura adecuado en cada unidad o gerencia.		
	Existe seguridad adecuada para el cableado en cada unidad o gerencia.		
	Existe mantenimiento de equipo en cada unidad o gerencia.		
	Existe verificación de seguridad del equipo fuera del local en cada unidad o gerencia.		
	Se comprueba eliminación segura o rehusó del equipo en cada unidad o gerencia.		
	Se comprueba el traslado de propiedades en cada unidad o gerencia		
Gestión de la Comunicación y Operaciones	Realizan procedimientos de operación debidamente documentadas.		
	La gestión de cambio es verificada en cada unidad o gerencia.		
	Existe responsabilidades y deberes		
	Se verifica la separación de los medios de desarrollo y operacionales en cada unidad o gerencia.		
	Existe alguna entrega de servicios en cada unidad o gerencia.		
	Se comprueba monitoreo y revisión de los servicios de terceros.		
	Existe alguna gestión de la capacidad en cada unidad o gerencia.		

	Se comprueba la aceptación del sistema en cada unidad o gerencia del Gobierno Regional.		
	Existe algún control sobre Software maliciosos en cada unidad o gerencia del Gobierno Regional.		
	Se evidencia los controles contra códigos móviles		
	Existen evidencias de Backup o controles de la información.		
	Existe algún control de Red en cada unidad o gerencia del Gobierno Regional.		
	Se comprueba la seguridad de los servicios de Red.		
	Se verifica la gestión de los medios removibles en cada unidad o gerencia del Gobierno Regional.		
	Se comprueba la eliminación de medios en cada unidad o gerencia del Gobierno Regional.		
	Existe algún Procedimientos de los manejos de información		
	Se comprueba la seguridad de documentación del sistema en cada unidad o gerencia del Gobierno Regional.		
	Existen procedimientos y políticas de información y Software.		
	Se verifica el registro de acuerdos de intercambios.		
	Se comprueba medios físicos en tránsito en cada unidad o gerencia del Gobierno Regional.		
	Se verifican los mensajes electrónicos en cada unidad o gerencia del Gobierno Regional.		
	Existe algunos sistemas de información comercial en cada unidad o gerencia del Gobierno Regional.		
	Existe verificación de registro de comercio electrónico en cada unidad o gerencia del Gobierno Regional.		
	Se comprueba Transacciones en línea		
	Se verifica la información disponible públicamente en cada unidad o gerencia del Gobierno Regional.		

	Existe algún Registro de auditoria en cada unidad o gerencia del Gobierno Regional.		
	Se verifica la existencia del sistema de monitoreo.		
	Existe alguna protección del sistema de monitoreo en cada unidad o gerencia del Gobierno Regional.		
	Se vírica la protección de la información del registro en cada unidad o gerencia del Gobierno Regional.		
Control de acceso	Se comprueba los registros del administrador y operador.		
	Existe algún Registro de fallas en cada unidad o gerencia del Gobierno Regional.		
	Existe verificación de sincronización de relojes.		
	Se comprueba las políticas del control de accesos en cada unidad o gerencia del Gobierno Regional.		
	Existe alguna inscripción del usuario en cada unidad o gerencia del Gobierno Regional.		
	Existe una verificación de gestión de privilegios en cada unidad o gerencia del Gobierno Regional.		
	Existe alguna gestión de clave de usuarios.		
	Revisión de los accesos de los derechos del usuario en cada unidad o gerencia del Gobierno Regional.		
	Existe algún uso de clave en cada unidad o gerencia del Gobierno Regional.		
	Equipamiento de usuario desatendido en cada unidad o gerencia del Gobierno Regional.		
	Existe alguna política de pantalla y escritorio limpio.		
	Existe alguna política sobre el uso de servicios en Red en cada unidad o gerencia del Gobierno Regional.		
	Se comprueba Autenticación del usuario para conexiones externas en cada unidad o gerencia del Gobierno Regional.		
	Se comprueba la identificación del equipo en Red en cada unidad o gerencia del Gobierno Regional.		

	Existe alguna protección del puerto de diagnóstico remoto.		
	Segregación en redes en cada unidad o gerencia del Gobierno Regional.		
	Existe algún control de conexiones en redes.		
	Se comprueba el control de routing en redes en cada unidad o gerencia del Gobierno Regional.		
	Existe algún procedimiento de registro en el terminal en cada unidad o gerencia del Gobierno Regional.		
	Se verifica la identificación y autenticación del usuario.		
	Se comprueba el sistema de gestión de claves en cada unidad o gerencia del Gobierno Regional.		
	Se verifica el uso de utilidades del sistema.		
	Existe alguna sesión inactiva.		
	Se comprueba la limitación de tiempo de conexión en cada unidad o gerencia del Gobierno Regional.		
	Existe alguna restricción al acceso a la información en cada unidad o gerencia del Gobierno Regional.		
	Existe algún aislamiento del sistema sensible en cada unidad o gerencia del Gobierno Regional.		
	Se verifica la existencia de computación móvil y comunicación en cada unidad o gerencia del Gobierno Regional.		
	Existe algún Teletrabajo en cada unidad o gerencia del Gobierno Regional.		

VALORACIÓN DE ACTIVOS

En cuanto a la valoración de los activos, se consideró la siguiente tabla:

VALOR	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
1	Se puede difundir, es de dominio público, todos los usuarios tienen acceso	Se puede tolerar que no esté disponible al menos una semana	Los errores o modificaciones no autorizadas no generan impacto en las unidades o gerencias y en el Gobierno Regional
2	Restringido para uso interno, si se filtra no ocasiona riesgo	Se puede tolerar que no esté disponible al menos un día	Los errores o modificaciones no autorizadas generan impacto leve en las unidades o gerencias y en el Gobierno Regional
3	Protegido es necesario controles para su acceso, si se filtra ocasiona riesgo moderado en las unidades o gerencias y en el Gobierno Regional	Se puede tolerar que no esté disponible al menos una hora	Los errores o modificaciones no autorizadas generan impacto moderado en las unidades o gerencias y en el Gobierno Regional
4	Confidencial, información muy sensible, si se filtra se ocasiona un daño grave a la en las unidades o gerencias y en el Gobierno Regional	No se tolera que el activo no se encuentre disponible	Los errores o modificaciones no autorizadas generan impacto critico en las unidades o gerencias y en el Gobierno Regional

PROBABILIDAD DE OCURRENCIA

Se debe establecer la probabilidad de ocurrencia de la amenaza relacionados con la seguridad de hardware y software en función de lo indicado en la siguiente tabla:

PROBABILIDAD DE OCURRENCIA

CATEGORIA	VALOR	DESCRIPCIÓN
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, se posee un muy alto grado de seguridad que ocurra en el año
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, se posee un alto grado de seguridad que ocurra en el año
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, se posee un moderado grado de seguridad que ocurra en el año
improbable	2	Riesgo cuya probabilidad de ocurrencia es baja se posee un bajo grado de seguridad que ocurre en el año
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja se posee un muy bajo grado de seguridad que ocurra en el año

NIVEL DEL RIESGO

IMPACTO		PROBABILIDAD DE OCURRENCIA				Total
		Muy rara vez	Hasta dos veces al Año	Hasta una vez al mes	Más de una vez al mes	
	Menor	8	0	51	0	59
	Significativo	25	7	1	0	33
	Dañino	2	0	15	0	17
	Serio	0	0	0	4	4
		35	**7**	**67**	**4**	**113**

MAGERIT V3:

ANÁLISIS DE RIESGOS

En esta fase se tienen que analizar los riesgos en cada una de las unidades o gerencias del Gobierno Regional de Ancash:

- ✓ Ejecutar inventario de hardware software y personal a cargo de la seguridad de la información y usuarios
- ✓ **E**xaminar los riesgos a los que está expuesto el hardware en las unidades o gerencias y en el Gobierno Regional
- ✓ Hacer análisis exhaustivo de las vulnerabilidades en las unidades o gerencias y en el Gobierno Regional

- ✓ Estudiar los conocimientos de los usuarios en función a la seguridad de la información en las unidades o gerencias y en el Gobierno Regional
- ✓ Examinar el riesgo existente cuando hacen uso de la nube y las redes sociales.
- ✓ Analizar la gestión de la seguridad actual respecto a cómo están identificando los riesgos, las vulnerabilidades, que conocimiento disponen sobre los ataques y los niveles de protección con los que cuentan en las unidades o gerencias y en el Gobierno Regional.
- ✓ Analizar el nivel se seguridad de la información, específicamente a los archivos más importantes en función a los atributos de disponibilidad, integridad y confidencialidad.

TRATAMIENTO DE RIESGOS

En este apartado se debe realizar el análisis de cada una de las unidades o áreas en las unidades o gerencias y en el Gobierno Regional en relación a las normas de seguridad de la información que están aplicando, los medios tecnológicos que dispone la institución gubernamental para enfrentar los riesgos; cómo están utilizando los medios de control de riesgos.

Analizar los conocimientos que los empleados usuarios del sistema información dispones respecto a la seguridad de la información, se va analizar los dominios sobre uso de hardware, software, seguridad e la información, etc.

SELECCIÓN DE SALVAGUARDAS

En esta fase se tiene que realizar los siguiente:

Analizar los mecanismos de control que están realizando los usuarios en las unidades o gerencias y en el Gobierno Regional

Examinar los controles en la seguridad de hardware, software y conocimiento de los usuarios aspecto a la seguridad de la información las unidades o áreas en las unidades o gerencias y en el Gobierno Regional.

Controlar la seguridad de los archivos informáticos de alta confidencialidad, así como también de hardware y software.

METODOLOGÍA

Se propone utilizar el estándar ISO/IEC 27001, cuyas fases son las siguientes:

PERFILES DEL MARCO DE SEGURIDAD ISO/IEC 27001

Respuesta ante incidentes de seguridad

Los usuarios de cada una de las unidades o gerencias del Gobierno Regional de Ancash que utilizan el sistema de información deben estar mentalizados de que los incidentes y accidentes que puedan ocurrir con relación a la seguridad de la información pueden ocurrir en cualquier momento, es por ello, que todos los empleados deben estar alertas y bien preparados para poder asegurar la integridad, confidencialidad y accesibilidad a la información sensible de las unidades o gerencias del Gobierno Regional de Ancash. En el caso de presentarse un ataque robo de información sensible para la institución, una de las acciones más básicas, es que el usuario deba desconectar su equipo de cómputo del sistema de información, rápidamente debe comunicar al área informática del incidente ocurrido mediante documentación. luego todos los empleados involucrados deben unir esfuerzos para responder los ataques. Cuando el ataque ha sido repelido se debe asegurar la inexistencia de seguridad, para luego proceder a una nueva conexión al sistema de información.

Todos los ataques al sistema de información deben ser registrados, mejor aún si se generan reportes estadísticos con frecuencia, incluso los pequeños fallos y errores espera sufrir el sistema de información y la información sensible deben ser reportados a la autoridad correspondiente le corresponde al área de informática validar los informes y explicar lo sucedido.

El informe que se presente a la autoridad competente debe contener el área en dónde ocurrió el incidente, personal y equipo de cómputo atacado, fecha y hora en qué ha ocurrido el ataque o falla, descripción de los ataques, errores o problemas presentados, describir cómo se solucionaron los problemas, o cómo se dieron respuesta al incidente materia de la comunicación, indicar la fecha y hora en que se dio solución al problema, si es posible indicar ciertas recomendaciones.

Es recomendable que las autoridades competentes de la institución gubernamental deban revisar periódicamente los informes que han sido registrados y corresponden a las fallas o ataques al sistema de información, deben estudiar los problemas y las soluciones alcanzadas, incluso estos incidentes deben ser materia de capacitaciones futuras.

Control de información

El control de información debe llevarse a cabo con tres niveles, nivel de hardware, software y a nivel de personal; a nivel de hardware, se deben controlar las unidades de almacenamiento, unidades de respaldo, nivel de protección del hardware, nivel de protección del servidor; es recomendable que estas unidades puedan disponer etiquetas que indiquen el proceso de control realizado.

El control también debe realizarse antes durante y después de la transmisión de información sensible o clasificada, debe tenerse en cuenta a quién se está destinando la información, se debe asegurar que quien envía la información es el que tiene el acceso, y asegurarse que la información ha sido cambiada o manipulada, es decir mantiene su integridad. Es recomendable que la autoridad que da acceso al personal a información sensible debe generar un documento para un mejor control.

Aunque las técnicas de encriptación son complejas, un grupo de empleados deben ser capacitados en técnicas de encriptación para garantizar la seguridad de la información dimensiones de integridad, accesibilidad y confidencialidad. Cuando un archivo o información sensible es transmitido o enviado a un destinatario debe tener la etiqueta de las dimensiones indicadas. Toda información sensible o

clasificada para la institución debe estar documentado en función a quiénes pueden acceder, a quienes se debe transmitir o enviar, en dónde se debe de almacenar, y se debe determinar el número de veces de copia de respaldo que debe tener para garantizar su plena seguridad.

Toda información que se genera en la institución, tales como archivos lógicos y físicos, documentos internos y externos, archivos e información recibida, archivos e información generada, etc., deben ser registrados en diversos repositorios, de preferencia en diferentes instalaciones, lo más óptimo, es almacenarlo en la nube, aunque implique costos para la municipal. El acceso a información clasificada o confidencial solo debe ser permitido para el empleado personal debidamente autorizado, para el caso de los registros físicos, el personal de seguridad difusión denominado vigilancia se responsabiliza del cuidado de la información física qué obra en poder de la institución. El personal que usa el sistema de información y que se encarga de la información clasificada sensible debe almacenar sus archivos, de preferencia con claves profesionales, esto significa y el tamaño de código o clave debe ser mayor igual a 12 caracteres que involucren, números, carácter alfanumérico, caracteres especiales, etc. deben evitar claves comunes en donde se usen fecha de nacimiento, iniciales de nombres y apellidos, etc., así como dar claves a sus compañeros de trabajo.

Intercambios de información y correo electrónico

El personal que usa el sistema de información y que está a cargo de la información sensible, cuando usa cualquier medio de correo electrónico, debe hacerlo solo para uso institucional, teniendo en cuenta los diversos ataques que puede recibir interna y externamente por este medio. El personal debe evitar enviar correos a destinos que considera no confiable, el personal tiene la responsabilidad de usar el correo electrónico específicamente para envío y recepción de información de autoridades debidamente registradas de la institución, no debe usar el correo electrónico para actividades que estén reñidas con la ética y la moral, actividades que no se

relacionan con las funciones y servicios que presta el Gobierno Regional de Ancash, así como también no deben divulgar su dirección de correo, excepto, a las autoridades de esta institución gubernamental.

Las mismas consideraciones que se debe tener para el uso de correo electrónico, el usuario también debe tenerlo presente para el uso de las redes sociales. El uso de las redes sociales y de los correos electrónicos pueden realizarse fuera de la institución, lo cual puede generar riesgos a la seguridad de la información, en ese sentido, el personal pertinente debe establecer controles adecuados en el uso de estos medios que utilizan como plataforma el internet. Para llevar un adecuado control en el uso de estos medios se deben revisar controles de forma periódica a los equipos, tales como celulares, computadoras, laptop, Tablet o cualquier otro medio electrónico que posibilita el intercambio de información. la impresión de la información clasificada o sensible debe ser impresa con conocimiento menos de las autoridades correspondientes, almacenamiento debe de realizarse en las mismas condiciones.

Seguridad de instalaciones de procesamiento de datos

Uno de los sistemas vulnerables ante ataques internos y externos son las instalaciones del sistema de información, es por ello que personal debe adoptar medidas de protección muy consistentes impertinentes, la seguridad debe estar en función de la clasificación de la información en función a su cantidad y valor, debido a que los atacantes realizan que estas actitudes porque dicho valor les genera un interés para configurar sus ataques; es por ello que la seguridad de las instalaciones del procesamiento de datos debe estar necesariamente restringido únicamente para el empleado o personal que ha sido autorizado mediante documentación.

Con la finalidad de garantizar la seguridad, los empleados de las unidades o gerencias del Gobierno Regional de Ancash deben ser visibles a sus puestos de trabajo, esto significa que deben portar un carnet o algún medio de identificación para que se le reconozca como tal, en la medida de lo posible la institución

gubernamental puede instalar sistema de control de seguridad, tales como videocámaras, sistemas de monitoreo, que permitan el control del personal interno en el acceso a los activos de información. La movilidad de algún sistema de información de una unidad a otra puede ser comunicada previamente mediante documentación a la autoridad correspondiente. Se debe tener un registro del personal que tiene acceso hay información clasificada, la cual debe ser generada por el área o unidad de las unidades o gerencias del Gobierno Regional de Ancash.

Administración de comunicaciones y operaciones

Las comunicaciones que se realizan en la institución gubernamental son de diversas formas, así como también los destinatarios de la información varían según el proceso de atención. La administración de la comunicación que implica el tratamiento de la información clasificada o confidencial debe estar a cargo del personal encargado, buenas sugerencias y la gerencia de cada en donde se genera la información confidencial. Los procesos operativos, así como las responsabilidades de acceso a la información confidencial o clasificada son considerados como actividades operativas de los empleados de las unidades o gerencias del Gobierno Regional de Ancash.

Los procesos de operación que implican trabajar con los sistemas de información clasificados y la información en general tienen que ser documentados, cualquier cambio en los procesos o actividades, necesariamente tienen que ser autorizados por la gerencia subgerencia correspondiente. La documentación generada de contener al personal involucrado, destino de información, tiempo en que se inicia el proceso, tiempo de duración del proceso, descripción de errores, fallas, riesgos, etc. Cualquier cambio operacional o metodológico que se pueda realizar en la generación de la documentación de la institución deben quedar establecidos y comunicados, al respecto, se exceptúan, a las informaciones o comunicaciones implique emergencias, los demás tipos de información deben seguir los procedimientos que ya han sido establecidos.

Protección contra virus

Generalmente los medios de ataques externos tienen como fundamento a los programas de virus enviados por uno o más atacantes, al respecto es responsabilidad de la unidad de informática, así como de los propios usuarios, específicamente quienes tienen a cargo información sensible, desarrollar todos los esfuerzos para repeler cualquier tipo de ataque externo. Los ataques que implican virus informático generalmente atacan a todas las unidades diarias de la empresa, es por ello que se hace necesario que los empleados llegan a estar capacitados para retener dichos ataques. Estos tipos de ataques son repelidos mediante el uso the software antivirus, para ello el personal debe conocerlo y aplicarlo de manera profesional, una de ellas consiste en que el programa debe estar configurado para que detecte en tiempo real cualquier tipo de ataque informal. Es necesario que se deba proveer de un sistema de protección contra ataques informáticos masivos, así como las capacitaciones correspondientes.

Control de acceso de datos

El acceso a la información y a los datos de las unidades o gerencias del Gobierno Regional de Ancash deben estar controlados para que se tenga la seguridad de que los usuarios están haciendo uso correcto de su función laboral, este control implica qué el sistema informático debe ser protegida contra las modificaciones de la información y los datos que no han sido autorizados. Quién controle el sistema de información debe hacer uso inteligente de la actividad de control de acceso para que pueda reducir la probabilidad de que cualquier usuario o atacante puede ingresar al sistema sin previa autorización. Cada empleado que use una computadora de la institución tiene que ser identificado, puede disponer de acceso único, debe controlar su actividad laboral, así como también con frecuencia debe ser monitoreado y comunicado con informe a la autoridad pertinente de las unidades o gerencias del Gobierno Regional de Ancash.

Es necesario que cada empleado tenga una clave de acceso y que no debe comunicar a nadie dicha clave. Cuando un usuario, con motivos justificados, abandona su

espacio de trabajo, la computadora debe ser configurada para que no permita el uso por otro usuario. En caso de despido del personal el acceso debe ser retirado o bloqueado inmediatamente.

El sistema de información de las unidades o gerencias del Gobierno Regional de Ancash, específicamente las computadoras y los procesos que realizan cada uno de los empleados que generan información deben ser auditados en función de la seguridad que brindan a la información, específicamente en información sensible. El área de informática debe controlar periódicamente el uso del sistema de información y generar los reportes personalizados por cada usuario, teniendo en cuenta la hora y fecha de la auditoría realizada.

Seguridad de contraseñas

Uno de los espacios más vulnerables con respecto a la seguridad de un sistema de información es la seguridad de las claves o contraseñas, generalmente muchos usuarios no tienen una cultura de generación y gestión de las claves que utilizan para acceder al sistema de información de la institución, quién es ese sentido, se debe generar una cultura de gestión de contraseñas, en donde este permitido una norma sobre el tratamiento de las claves, lo básico es que se deben generar contraseñas que tengan un cierto nivel de complejidad, mínimo de un tamaño de 10 caracteres, en donde se combinen, caracteres alfanuméricos, numéricos, caracteres especiales, y la combinación de mayúsculas y minúsculas.

El uso de una contraseña no debe pasar de dos meses de uso, no debe compartirse con nadie, tampoco debe estar permitido cambiar contraseñas con los compañeros de trabajo, todos deben cuidar y proteger sus respectivas claves bajo responsabilidad, las contraseñas no deben ser accesibles incluso al entorno familiar, para poder recordar el código, estos deben ser almacenados en medios digitales con acceso solo al legítimo usuario. No se debe compartir la contraseña por ningún medio electrónico.

Las claves tampoco pueden ser utilizadas para acceder a otros entornos informáticos, eso significa que no debe usarse la misma clave para acceder a correos electrónicos propios o cualquier otro medio informático. Ningún empleado de la institución debe pedir o exigir la clave a su compañero de trabajo, a menos que sea necesario para realizar ciertos procesos, y esto debe ser solicitado por la autoridad competente. El uso de las claves o contraseñas es responsabilidad de cada usuario, es por ello que su gestión conlleva a responsabilidades y posibles sanciones.

Cada usuario no necesariamente maneja una sola clave de acceso, estas claves pueden ser creadas para ingresar al sistema general, se pueden crear claves para ponerlos a las carpetas de trabajo, a los archivos, específicamente a los que tienen información de importancia o sensible, etc., Como se puede observar, los empleados pueden gestionar varias claves, es su responsabilidad gestionarlos adecuadamente. En el caso de pérdida de las claves, el mismo sistema, dispone de los mecanismos informáticos para poder recuperarlos y cambiarlos; por otro lado, también puede existir la política de que las claves pueden ser guardadas y conocidas por el jefe de informática, o algún otro personal asignado documentadamente. Las claves también pueden ser vulneradas cuándo los usuarios comparten el mismo sistema de información, en este caso, debe estar normado que, cada trabajador debe usar solo su sistema de cómputo.

Las contraseñas implican una mejor gestión cuándo el usuario está a cargo de la gestión de información sensible y de importancia para la institución, en el caso de despido del personal, el área correspondiente debe destinar directamente con el área de informática para que el acceso de mi usuario saliente deba ser eliminada. Los usuarios con privilegios acceder a información sensible deben ser controlados frecuentemente.

El jefe de área de informática, así como también los empleados a usuarios con acceso a cuentas en dónde se guarda información sensible o privilegiada, es necesario que deban tener cuentas personales para que puedan desarrollar sus funciones que no implican el desarrollo de sus privilegios. En el caso de que las

cuentas no se utilicen durante un tiempo considerable debe ser cerrado con la finalidad de dinero y los riesgos y vulnerabilidades para la seguridad del sistema de información. debe establecerse como política institucional de que todos los accesos al sistema de información de las unidades o gerencias del Gobierno Regional de Ancash se controlen usando la metodología de autenticación, lo cual debe incluir una combinación básica de identificación de usuario y clave de acceso, esta combinación tiene que garantizar y proveer la verificación de la identidad el usuario que desea acceder al sistema.

Puede suceder en el desarrollo de la gestión administrativa y operativa que más de un usuario puedan realizar tareas similares, en ese sentido, se hace necesario que se utilicen controles de acceso con el objetivo de dar permisos y accesos a las cuentas del usuario. Debe constituirse como política de que cada usuario debe tener un identificador único, y que esto sea validado para un tiempo específico considerado como el tiempo de contrato del usuario, estos identificadores solo deben ser utilizados por un miembro del grupo, Incluso cuando el titulara ya no trabaje en la institución o haya renunciado. se debe impedir el uso de sesiones múltiples para una sola tarea.

El sistema de información es, por ningún motivo, debe ser utilizado para el desarrollo de software o de negocios personales, o que estén alejados de la función administrativa, operativa y de servicio del Gobierno Regional de Ancash. Los usuarios deben estar prohibidos de usar el sistema de información para la elaboración de trabajos o documentación ajeno a la institución, por lo tanto, los empleados que no estén de acuerdo con las normas de seguridad de la información, tampoco deben tener acceso al sistema de información.

Control de acceso a redes

El desempeño de las funciones administrativas y operativas implica que los empleados puedan acceder a la red del sistema de información, el acceso inadecuado, puede representar riesgos y vulnerabilidades como consecuencia de su complejidad e interrelación entre los trabajadores de la institución. los usuarios

deben tener cuidado cuando acceden remotamente a la red del gobierno regional debido a que representan riesgos y vulnerabilidad. El acceso desde cualquier sistema de información hacia el sistema, deben ser controladas por un sistema de hardware denominado firewall con el propósito de evitar o prevenir accesos que no han sido autorizados. que nadie de informática tiene la responsabilidad de aprobar pon desaprobar conexiones con redes externas.

El acceso desde cualquier punto de internet hacia la red de la institución gubernamental de ser rechazado mediante mecanismos de autenticación o mediante el uso de contraseñas dinámicas. El ingreso hacia los datos e información debe implicar la solicitud de autenticación, estos son, conocimiento que hace referencia a lo que el usuario conoce, contraseña o clave, la cual puede hacerse mediante sistema biométrico con colocación de huella digital u ocular también denominado lectores de retina, también se puede usar sistema de identificación de voz como medio de acceso.

Las computadoras, cuando sea necesario, tienen que ser bloqueadas en el caso de algún tipo de ataque interno o externo, se deben revisar periódicamente las conexiones de red internas y externas, esta revisión implica el cumplimiento con la política de seguridad en función al control de acceso y servicios que presta el sistema de información, cada usuario debe acceder al sistema solamente con las claves o contraseñas que han sido otorgadas para tal fin, está prohibido crear nuevas contraseñas y utilizarlos sin avisar a la autoridad correspondiente.

El sistema de información del Gobierno Regional de Ancash siempre va a tener los servicios habilitados para que los usuarios puedan hacer uso de ella, con el acceso y el uso se generan riesgos concatenados a dichos servicios de red, las cuales deben ser siempre tenidos en cuenta para no dar espacios a futuros ataques que provengan de fuentes internas o externas. Los usuarios deben ser conscientes de dichas riesgos y vulnerabilidades, en ese sentido deben estar siempre preparados para aplicar sus conocimientos sobre seguridad de la información a niveles de software y hardware,

así como también comunicar a la autoridad correspondiente los incidentes y accidentes que pudieran acontecer.

Los usuarios que tienen acceso a información sensible y de importancia para la institución, deben siempre cuidar las características de la información, estos son, la integridad, la accesibilidad y la confidencialidad, los usuarios están prohibidos de acceder a áreas que no le corresponden y que deben estar restringidas para ellos, así como también hacer cualquier intento de conocer a la cifra las contraseñas de sus compañeros de trabajos, utilizar algoritmos que le permita acceder a dichas contraseñas, también se les prohíbe ingresar a medios de interacción social, tales como, correos electrónicos y redes sociales, y la propia internet, debido a que significan generación de riesgos y vulnerabilidades que se puedan generar durante la navegación.

Un factor muy importante en la generación de riesgos y vulnerabilidades es el acceso a internet cuando no se utiliza adecuadamente, debido a que es una ventana abierta a futuros ataques externos e internos, para contrarrestar este problema, se debe controlar y mejorar el sistema de cortafuegos el sistema de información. El acceso a internet debe estar normado controlado, con especial énfasis a los usuarios encargados de la seguridad y el manejo de información sensible y de importancia para el gobierno regional. Por otro lado, los usuarios solo deben ingresar a internet para realizar las labores propias, cualquier otro tipo de trabajo realizado en este medio por el usuario debe ser sancionado en función a lo establecido en la norma.

Control de acceso al sistema operativo

Cuando se desea dar seguridad al sistema de información, el acceso al sistema operativo de la red es un factor de vital importancia debido a que en este medio se configuran los diversos elementos de hardware para la protección frente a cualquier ataque que pueda poner en riesgo la seguridad de la información. En este caso, la administración de la red que está a cargo del área de informática debe otorgar privilegios específicos y pertinentes a cada uno de los usuarios en función a los rangos o jerarquías de sus cargos. Es necesario que cada uno de los usuarios deban

poseer solo un identificador, en caso de otorgar identificadores compartidos, esto debe ser autorizado previamente por la autoridad competente, los usuarios deben tener una contraseña a su cuenta de usuario, el dueño del identificador debe conocer esta contraseña.

Control de acceso de aplicación

Los usuarios del sistema de información del Gobierno Regional de Ancash siempre van a trabajar con software instalado por la misma institución, estos programas constituyen un conjunto de aplicaciones que sirven para la generación de la información todo nivel, en la configuración del perfil de usuario se deben asignar el uso de esas aplicaciones para cada usuario de acuerdo con las funciones que les toca desempeñar. Tal como sucede con el sistema operativo, el acceso a las aplicaciones por parte de los usuarios debe ser controlados periódicamente con la finalidad de garantizar la seguridad estaba el sistema, en ese sentido se debe asignar a cada uno de los usuarios el acceso a la información mínima para que puedan realizar sus tareas asignadas, para ello se pueden restringir el acceso a ciertas líneas de comando, se puede designar limitación de permisos información sensible o archivos de sistemas, asignarlos solo en modo lectura, se puede realizar adecuados controles con referencia a la información de entrada y salida, tal vez como generación de documentos, reportes, consultas, filtros, etc.

Las aplicaciones utilizadas, específicamente, aquellas aplicaciones que están relacionadas con la generación de información sobre proyectos de inversión pública, licitaciones de obras, liquidaciones de obras, generaciones de planes estratégicos, información crítica en general, deben disponer de hora y fecha regeneración y transmisión con la finalidad de generar líneas históricas de trazabilidad y para que esto pueda facilitar los procesos de auditoría interna o externa, los administradores de la red tiene la obligación de realizar los monitoreos de seguimiento y la generación y envío de estos tipos de información, también se debe controlar a los usuarios que utilizan estas aplicaciones. Cada usuario que genera información sensible y de importancia para el Gobierno Regional de Ancash

debe revisar periódicamente la integridad, confidencialidad y accesibilidad de los documentos que ha generado y enviado.

Seguridad respecto a computación móvil y teletrabajo

Un aspecto muy importante a tener en cuenta en estos tiempos eres la computación móvil y teletrabajo, en ese sentido, cada uno de los usuarios que utilizan esta modalidad de trabajo, también deben ser controlados sobre cómo están desarrollando sus actividades en función a la seguridad del sistema de información, en este caso los usuarios deben tener las mismas responsabilidades y consideraciones sobre la seguridad de información implementada por la institución gubernamental. En el caso de uso de aplicaciones de control remoto de cualquier elemento del sistema de información se debe prohibir su uso, a menos que disponga de la autorización de la administración del área de informática, el uso inapropiado de programas de acceso remoto puede propiciar ventanas abiertas de acceso a intrusos internos y externos para que pueda apropiarse de la información sensible.

Para el caso del trabajador remoto, las medidas adicionales de seguridad que se deben adoptar con fines de proteger la información, se deben incrementar los datos, quieren aplicar contraseñas de encendido, se debe realizar charlas de concientización a los usuarios sobre los riesgos y vulnerabilidades que implica el uso del sistema en la modalidad del trabajo remoto, se debe dar protección a la información desde y hacia los dispositivos móviles, así como también tomar medidas adicionales de autenticación con la finalidad de acceder al sistema de información.

Responsabilidades personales

El acceso y uso cotidiano del sistema de información acarrea responsabilidades personales para cada usuario debidamente autorizado, bajo estricta responsabilidad, los usuarios están prohibidos de revelar el identificador y contraseña a terceros, no deben escribirla y exponerla a la vista del entorno, por ningún motivo debe estar al alcance de sus compañeros de trabajo, asimismo los usuarios están prohibidos de

utilizar accesos o contraseñas de sus compañeros de trabajo, así dispongan de la autorización del propietario de la cuenta y contraseña. En el caso de que un usuario sospeche de qué se cuenta este siendo usado por algún compañero de trabajo, inmediatamente debe proceder al cambio de su contraseña, así como también informar rápidamente a la administración de la red para que tome conocimiento y proceda de acuerdo a lo normado.

Puede suceder que al sistema le pida al usuario el cambio automático de sus claves, en este caso, es recomendable que pueda cambiar sus claves con una frecuencia mensual, porque podría darse el caso en que el sistema podría denegarle el acceso con la consecuencia de pérdida de tiempo, y a que viniera a consultar con el administrador de la red para cambiar o solicitar nueva clave. Es responsabilidad del usuario proteger la información sensible del Gobierno Regional de Ancash teniendo en cuenta la tecnología y sus posibilidades, por ningún motivo deben hacer revelaciones sobre el contenido de la información sensible, tampoco deben modificar, destruir, borrar todo parte del contenido de la información. Cada uno de los usuarios tienen la autorización de crear archivos en función al perfil otro lado, así como también pueden crear archivos temporales siempre en cuando formen parte de su desempeño laboral.

Los usuarios están obligados de comunicar por escrito al administrador de la red del área de informática sobre cualquier tipo de riesgos y vulnerabilidades que presente el sistema en dónde se desempeña, así como también deben informar sobre las incidencias que puedan poner en riesgo la seguridad de los datos e información, cualquier sospecha de uso no legítimo de la información y acceso no autorizado por terceras personas deben ser comunicadas inmediatamente.

Uso apropiado de los recursos

Los recursos tecnológicos o informáticos, tales como información, datos, software, hardware, supresoras, servidores, entre otros elementos de hardware, siempre deben estar disponibles para el usuario, para que puedan cumplir satisfactoriamente su respectivo desempeño laboral, así como los objetivos que ha sido debidamente

planificados. Los usuarios que utilizan estos recursos están sujetos a controles y monitoreos con la finalidad de garantizar la seguridad de los recursos, en ese sentido se prohíbe el uso de dichos recursos un funciones o actividades que no sean lo que la institución desarrolla, asimismo se prohíben las instalaciones de software sin previo consentimiento de la autoridad competente.

El área de informática debe comunicar a los usuarios sobre la prohibición de la introducción de sistema de información, software, hardware o contenidos reñidos con la ética y la moral, así como también contenidos ofensivos y amorales al sistema informático. Cuando el usuario desea instalar algún software de cualquier tipo, debe comunicar a la autoridad correspondiente, que en este caso recae a la Jefatura del área informática. Tampoco le está permitido descargar sistemas para poder ser archivados en las computadoras, cuando eso se desea, debes solicitar un permiso a la autoridad correspondiente.

Los usuarios, específicamente los que están a cargo de la información sensible que confidencial del Gobierno Regional de Ancash están prohibidos de alterar o cambiar, destruir, borrar cualquier tipo de dato, información o documentación física y electrónica. El dar de baja a archivos de importancia para la institución deben estar debidamente justificados, tal como ocupación innecesaria despacio en la unidad de almacenamiento, obsolescencia de la información, etc. Los programas antivirus solamente son instalados por el personal asignado por el área informática, en ese sentido los usuarios están prohibidos de instalar cualquier tipo de software legal o ilegal, incluso aquellos softwares que la institución la adquirido con licencia. los usuarios están prohibidos de cargar programas qué pueden significar obstrucción y retraso en el desarrollo del desempeño laboral, o que pudieran dañar los elementos del sistema de información.

REPOSITORIO INSTITUCIONAL DIGITAL

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE DOCUMENTOS DE INVESTIGACIÓN

1. Información del Autor		
GONZALES TORRES JACKSON JUNIOR	71340219	jackson.gt.95@gmail.com
Apellidos y Nombres	**DNI**	**Correo Electrónico**

2. Tipo de Documento de Investigación							
X	Tesis		Trabajo de Suficiencia Profesional		Trabajo Académico		Trabajo de Investigación

3. Grado Académico o Título Profesional [1]									
	Bachiller	X	Título Profesional		Título Segunda Especialidad		Maestría		Doctorado

4. Título del Documento de Investigación

Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023

5. Programa Académico

Ingenieria Informatica y de Sistemas

6. Tipo de Acceso al Documento			
X	Abierto o Público [3] (info:eu-repo/semantics/openAccess)		Acceso restringido [4] (info:eu-repo/semantics/restrictedAccess) (*)
	Embargo (Máximo 24 meses) (info:eu-repo/semantics/embargoedAccess)	Fecha de Liberación de embargo: _____ / _____ / _____ (Formato: día / mes / año)	
(*) En caso de restringido y embargo sustentar motivo			

A. Originalidad del Archivo Digital

Por el presente dejo constancia que el archivo digital que entrego a la Universidad, es la versión final del trabajo de investigación sustentado y aprobado por el Jurado Evaluador y forma parte del proceso que conduce a obtener el grado académico o título profesional.

B. Otorgamiento de una licencia CREATIVE COMMONS [5]

El autor, por medio de este documento, autoriza a la Universidad, publicar su trabajo de investigación en formato digital en el Repositorio Institucional Digital, al cual se podrá acceder, preservar y difundir de forma libre y gratuita, de manera íntegra a todo el documento. [6]

Ciudad	Día	Mes	Año
Huaraz	20	05	2024

Huella Digital

Firma

Importante

1. Según Resolución de Consejo Directivo N° 033-2016-SUNEDU-CD, Reglamento del Registro Nacional de Trabajos de Investigación para optar Grados Académicos y Títulos Profesionales, Art. 8, inciso 8.2.
2. Ley N° 30035. Ley que regula el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto y D.S. 006 -2015-PCM.
3. Si el autor eligió el tipo de acceso abierto o público, otorga a la Universidad San Pedro una licencia no exclusiva, para que se pueda hacer arreglos de forma en la obra y difundir en el Repositorio Institucional Digital. Respetando siempre los Derechos de Autor y Propiedad Intelectual de acuerdo y en el Marco de la Ley 822.
4. En caso de que el autor elija la segunda opción, únicamente se publicará los datos del autor y resumen de la obra, de acuerdo a la directiva N° 004-2016-CONCYTEC-DEGC (Numerales 5.2 y 6.7) que norma el funcionamiento del Repositorio Nacional Digital
5. Las licencias Creative Commons (CC) es una organización internacional sin fines de lucro que pone a disposición de los autores un conjunto de licencias flexibles y de herramientas tecnológicas que facilitan la difusión de información, recursos educativos, obras artísticas y científicas, entre otros. Estas licencias también garantizan que el autor obtenga el crédito por su obra.
6. Según el inciso 12.2, del artículo 12° del Reglamento del Registro Nacional de Trabajos de Investigación para optar grados académicos y títulos profesionales -RENATI "Las universidades, instituciones y escuelas de educación superior tienen como obligación registrar todos los trabajos de investigación y proyectos, incluyendo los metadatos en sus repositorios institucionales precisando si son de acceso abierto o restringido, los cuales serán posteriormente recolectados por el Repositorio Digital RENATI, a través del Repositorio ALICIA".

Nota. - En caso de falsedad en los datos, se procederá de acuerdo a ley (Ley 27444, art. 32, núm. 32.3).

Plan de mejora de la seguridad de la información aplicando estándar ISO/IEC 27001 en el Gobierno Regional de Ancash, 2023

INFORME DE ORIGINALIDAD

21%	21%	6%	8%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorio.ucv.edu.pe Fuente de Internet	2%
2	repositorio.uladech.edu.pe Fuente de Internet	1%
3	repositorioacademico.upc.edu.pe Fuente de Internet	1%
4	repositorio.unheval.edu.pe Fuente de Internet	1%
5	hdl.handle.net Fuente de Internet	1%
6	repositorio.upao.edu.pe Fuente de Internet	1%
7	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
8	www.regionayacucho.gob.pe Fuente de Internet	1%

9	qdoc.tips Fuente de Internet	1 %
10	1library.co Fuente de Internet	1 %
11	www.regionjunin.gob.pe Fuente de Internet	1 %
12	repositorio.untels.edu.pe Fuente de Internet	1 %
13	moam.info Fuente de Internet	<1 %
14	repositorio.unsch.edu.pe Fuente de Internet	<1 %
15	repositorio.undac.edu.pe Fuente de Internet	<1 %
16	repositorio.unapiquitos.edu.pe Fuente de Internet	<1 %
17	repository.unad.edu.co Fuente de Internet	<1 %
18	www.mef.gob.pe Fuente de Internet	<1 %
19	www.estrategia.gobiernoenlinea.gov.co Fuente de Internet	<1 %
20	Submitted to Universidad Privada San Pedro Trabajo del estudiante	<1 %

21	revistas.urp.edu.pe Fuente de Internet	<1 %
22	rraae.cedia.edu.ec Fuente de Internet	<1 %
23	repositorio.usanpedro.edu.pe Fuente de Internet	<1 %
24	cybertesis.unmsm.edu.pe Fuente de Internet	<1 %
25	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1 %
26	repositorio.utp.edu.co Fuente de Internet	<1 %
27	tesis.pucp.edu.pe Fuente de Internet	<1 %
28	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1 %
29	www.bdigital.unal.edu.co Fuente de Internet	<1 %
30	repositorio.udh.edu.pe Fuente de Internet	<1 %
31	dominiodelasciencias.com Fuente de Internet	<1 %

32	www.regionlambayeque.gob.pe Fuente de Internet	<1 %
33	inba.info Fuente de Internet	<1 %
34	Submitted to Universidad Alas Peruanas Trabajo del estudiante	<1 %
35	Submitted to Universidad Señor de Sipan Trabajo del estudiante	<1 %
36	repositorio.uigv.edu.pe Fuente de Internet	<1 %
37	www.regionsanmartin.gob.pe Fuente de Internet	<1 %
38	fr.slideshare.net Fuente de Internet	<1 %
39	www.scribd.com Fuente de Internet	<1 %
40	info.undp.org Fuente de Internet	<1 %
41	www.regionhuancavelica.gob.pe Fuente de Internet	<1 %
42	documentop.com Fuente de Internet	<1 %
43	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1 %

44	Submitted to Universidad Abierta para Adultos Trabajo del estudiante	<1 %
45	ojs.focopublicacoes.com.br Fuente de Internet	<1 %
46	regionayacucho.gob.pe Fuente de Internet	<1 %
47	Submitted to Universidad Tecnológica Centroamericana UNITEC Trabajo del estudiante	<1 %
48	cdn.www.gob.pe Fuente de Internet	<1 %
49	tesis.unap.edu.pe Fuente de Internet	<1 %
50	www.repositorio.usanpedro.edu.pe Fuente de Internet	<1 %
51	ausschreibungen.dgmarket.com Fuente de Internet	<1 %
52	Submitted to uncedu Trabajo del estudiante	<1 %
53	www.protivitiuniversityperu.com Fuente de Internet	<1 %
54	www.regionlima.gob.pe Fuente de Internet	<1 %

55	dspace.espoch.edu.ec Fuente de Internet	<1 %
56	dspace.utb.edu.ec Fuente de Internet	<1 %
57	gc.scalahed.com Fuente de Internet	<1 %
58	www.bsigroup.com Fuente de Internet	<1 %
59	www.escuelaeuropeaexcelencia.com Fuente de Internet	<1 %
60	www.isotools.org Fuente de Internet	<1 %
61	www.regionmadrededios.gob.pe Fuente de Internet	<1 %
62	doku.pub Fuente de Internet	<1 %
63	dpc-rivista-trimestrale.criminaljusticenetwork.eu Fuente de Internet	<1 %
64	repositorio.espe.edu.ec:8080 Fuente de Internet	<1 %
65	repositorio.puce.edu.ec Fuente de Internet	<1 %
66	repositorio.unjfsc.edu.pe	

Fuente de Internet

<1 %

67	repositorio.upn.edu.pe Fuente de Internet	<1 %
68	worldwidescience.org Fuente de Internet	<1 %
69	www.iesrioverde.es Fuente de Internet	<1 %
70	www.mpconsultores.com Fuente de Internet	<1 %
71	www.researchgate.net Fuente de Internet	<1 %

Excluir citas	Apagado	Excluir coincidencias	< 10 words
Excluir bibliografía	Activo		