UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN GESTIÓN PÚBLICA

Percepción de la implementación de la NTP-ISO/IEC 27001:2014 en base a la información documentada del gobierno central del Perú, año 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Gestión Pública

AUTORA:

Diaz Lara, Vanessa Liliana (ORCID: 0000-0001-7262-1007)

ASESOR:

Dr. Ramírez Ríos, Alejandro (ORCID: 0000-0003-0976-4974)

LÍNEA DE INVESTIGACIÓN:

Reforma y Modernización del Estado

LIMA – PERÚ

2021

Dedicatoria

A Dios, quién guía mi camino y me motiva a continuar preparándome para cumplir el propósito de servir a mi prójimo a través del servicio público.

A mis amados y abnegados padres Juan Gustavo Diaz Polanco y Teodolinda Lara Giraldo de Diaz por todo su amor, ejemplo y apoyo incondicional.

Agradecimiento

A mis exjefes: Joan Palacios y Rosa Cerna por alentarme a iniciar mi maestría en Gestión Pública.

A Patricia Valdivia, Serafín Álvarez, Franco Gamboni, Fernando Soriano y Elvis Malpartida por ser mi apoyo en el aprendizaje y práctica de la norma ISO/IEC 27001.

A mi familia, amigos, hermanos de la fe, compañeros de la maestría; por su amor, confianza, apoyo espiritual y apoyo académico respectivamente, sin ustedes no hubiera podido iniciar, cursar y culminar esta maestría.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

El presente estudio de investigación tiene como finalidad medir la percepción de la implementación de la NTP ISO/IEC 27001:2014, teniendo como referencia la información documentada que establece la norma, los documentos que determinen o vengan usando las entidades del gobierno central del Perú.

La metodología de investigación seleccionada ha sido de enfoque cuantitativo y de tipo descriptivo simple, considerando que está orientada a mostrar los resultados de las dimensiones de las variables: Planificación (Planear), ejecución(hacer), verificación(verificar) y mejora continua(actuar) con un horizonte de tiempo al cierre del año 2020. La población asciende a un total de 76 servidores públicos, quienes ejercen funciones relacionadas a la gestión de las TI y seguridad de la información e informática en las entidades que conforman los 19 sectores del poder ejecutivo en el nivel de gobierno central; asimismo, se empleó una muestra censal y se aplicó una encuesta con 40 pregunta cerradas de la escala ordinal. Las preguntas se encuentran alineadas a los instrumentos de gestión, marco normativo en materia digital y plataformas tecnológicas vigentes en el sector público; para ello, se obtuvo la validación de tres expertos de distintas especialidades, contándose con la respectiva confidencialidad mediante Alfa de Cronbach.

En los resultados obtenidos se determinó que alrededor del 50% de los encuestados perciben que la implementación de la NTP-ISO/IEC 27001:2014 en sus respectivas entidades es regular, con respecto a las dimensiones, el 42% de los encuestados percibió que la implementación de las cláusulas de Planificación es regular, el mismo nivel alcanzó la percepción de la implementación de las cláusulas de ejecución dado que el 58% de los encuestados así lo calificaron, con respecto a la implementación de las cláusulas de verificación fue percibida como buena 57%, con respecto a la mejora continua el mayor puntaje lo obtuvo el nivel regular dado que el 61% de los encuestados así lo consideraron.

Palabras claves: ISO 27001, PHVA, información documentada.

Abstract

The purpose of this research study is to measure the perception of the implementation of the NTP ISO / IEC 27001: 2014, taking as a reference the documented information established by the standard, the documents determined or used by the central government entities of Peru.

The research methodology selected has been of a quantitative approach and of a simple descriptive type, considering that it is oriented to show the results of the dimensions of the variables Planning (Plan), Doing (Do), Checking (Check) and continuous improvement (Act) with a time horizon at the end of the year 2020. The population amounts to a total of 76 public servants, they perform functions related to IT management and information security and computer security in the entities that make up the 19 sectors of the executive power in the level central government; as well, a census sample was used, and a survey with 40 closed questions of the ordinal scale was applied. The questions are aligned to the management instruments, regulatory framework in digital matters y current technology platforms in the public sector; for it, the validation of three experts from different specialties was obtained, the respective confidentiality was obtained using Cronbach's Alpha.

In the results obtained, it was determined that around 50% of those surveyed perceive that the implementation of the NTP-ISO/IEC 27001:2014 in their respective entities is regular, with regard to dimensions, 42% of those surveyed perceived that the implementation of the Planning clauses is regular, the same level reached the perception of the implementation of the execution clauses because 58% of those surveyed rated it that way, Regarding the implementation of the verification clauses, it was perceived as good 57%, regarding continuous improvement, the highest score was obtained by the regular level, because 61% of the respondents considered it that way.

Keywords: ISO 27001, PDCA, documented information.

I. INTRODUCCIÓN

Tras la tragedia del 11 de setiembre de 2001, la seguridad de la información viene siendo abordada con un gran sentido de urgencia por diversos organismos, entre ellos, la OCDE (2012); esto es, al haberse identificado que muchas empresas con sedes en las torres gemelas de Nueva York no pudieron reanudar sus operaciones por no haber contado con medidas necesarias que aseguren tener la disponibilidad de su información tras un escenario de desastre. Añadiendo a ello, la masificación del uso de las tecnologías de la información - TI, el aumento de la producción de información digital y la intensificación de la ciberdelincuencia, evidencia la problemática de encontrarnos ante técnicas de ataques informáticos cada vez más sofisticadas Carvalho y Marques (2019), mostrando lo vulnerable que se encuentran las organizaciones. En esa línea, PWC (2019) en una encuesta realizada en el año 2018, entrevistan a 9,500 personas de gestión y gobierno de las TI en 122 países; quienes indicaron que la pérdida de datos sensibles y la interrupción de operaciones son las principales consecuencias de los ataques informáticos que tuvieron que afrontar, con pérdidas de US$ 4,8 millones anuales aproximadamente.

Por otra parte, el FEM (2020) advierte que los ciberataques son los riesgos con mayores probabilidades de suceder; siendo la tercera causa de mayor preocupación; y que la falta de privacidad de los datos es considerado como un obstáculo del desarrollo de la economía digital; respaldando lo precitado, la INTERPOL(2020) advierte que la ciberdelincuencia ha tenido un incremento exponencial, manifestándose a través de la creación de sitios web falsos relacionados con la COVID-19, la difusión masiva de mecanismos de captura de datos personales para la usurpación de identidad; la cual llegó a tener alrededor de un millón de mensajes de correo basura relacionados con el coronavirus entre enero y abril de 2020. Asimismo, según Malwarebytes (2019), el secuestro de información, conocido como ransomware, es la modalidad de ataque con mayor incremento en la Unión Europea, aumentó un 200% durante el año 2019. Existen también, escenarios no intencionados, como los desastres o eventos que pueden perjudicar la confidencialidad,

integridad y disponibilidad, por ejemplo, actualmente, a consecuencia del COVID-19, la masificación del teletrabajo ha obligado a las organizaciones a abrir los controles de seguridad de su información clasificada como confidencial, exponiéndola ante nuevas amenazas y riesgos que podrían ocasiones su pérdida.

En el aspecto individual, es sorprendente que tras décadas de la masificación de internet la contraseña más usada en el mundo continúe siendo la cadena de texto “123456”, tal como lo reporta el Centro de Ciberseguridad nacional del Reino unido, NCSC (2019), y, que al ser de fácil descifrado puede significar una situación de inseguridad de los datos personales e información digital.

En América Latina y el Caribe, de acuerdo al estudio por la Organización de Estados Americanos – OEA en conjunto con el Banco Interamericano de Desarrollo – BID(2020), las tendencias del uso de las tecnologías de la información y la comunicación - TIC están en constante crecimiento, presionando a los gobiernos y empresas privadas la responsabilidad de generar la confianza por parte de los ciudadanos y usuarios en el ecosistema digital; no obstante el panorama en esta región del mundo, no resulta alentador, dado que desde el año 2016 a la fecha, solamente cuatro países se han adherido al Convenido de Budapest, conocido como el Convenio sobre Cibercrimen del Consejo de Europa. Ello, se puede evidenciar en los resultados del reporte anual por una de las empresas líderes en protección antivirus ESET (2019); en donde se reporta para el año 2018, el 61% de las empresas de América Latina tienen mayor preocupación por el acceso indebido, tras ello, se encuentra el robo de información con un 58%; en dicho estudio también se muestra que dos (02) de cada cinco (05) empresas de Latinoamérica sufrieron una infección de código malicioso, también conocido como malware o virus informático.

Según el precitado reporte de ESET, en el 2018, el Perú ha sido el país más afectado de la región en ataques de secuestro de información y el segundo, tras el país de México, en explotación de vulnerabilidades; en ese sentido, la Secretaría de Gobierno Digital – como ente rector en Gobierno Digital, inició el proceso de generar la confianza de los ciudadanos y demás

usuarios de los servicios digitales tanto en las empresas públicas como privadas, proceso que se ha iniciado con el Decreto de Urgencia N° 007-2020, sin embargo, tras ello, se tiene poca o ninguna información del grado de implementación de la Norma Técnica Peruana ISO/IEC 27001:2014, PCM(2014) en las entidades del Sistema de Transformación Digital, ésta última creado con Decreto de Urgencia N° 006-2020.

Desde el 16 de marzo de 2020, mediante el Decreto de Urgencia N° 026-2020, se declara el inicio de la emergencia sanitaría y mediante el Decreto Supremo Nº 010- 2020-TR se establece el trabajo remoto, obligando al aparato público estatal a reconfigurarse a fin de continuar con sus operaciones diarias bajo un escenario no visto antes; percibiéndose la carencia de medidas que aseguren la confidencialidad, integridad y disponibilidad de la información institucional relacionada a sus procesos internos y a los servicios que se brindan a la ciudadanía y administrados en general.

En el caso del poder ejecutivo, específicamente en el nivel de gobierno central, del total de los diecinueve sectores que lo conforman, se desconoce el nivel de implementación, siendo escasas las entidades públicas que han culminado las fases de implementación conforme al estándar internacional ISO 27001; evidenciándose que en su gran mayoría solo reportan la conformación del Comité de Gobierno Digital, la designación del Oficial de Seguridad de la Información y la Política de Seguridad de la Información, tal como se puede apreciar en sus respectivos Portales de Transparencia; por lo que no se puede medir de manera tangible el grado de madurez de la implementación del SGSI en las entidades que conforman cada uno de los sectores.

De acuerdo con lo descrito nos planteamos como problema de investigación ¿Cuál es el nivel de la percepción de la implementación de la NTP ISO/IEC-27001:2014 en base a la información documentada del gobierno central del Perú? Asimismo, nos planteamos los problemas específicos: (a)¿Cuál es el nivel de la percepción de la implementación de las cláusulas de planificación de la NTP ISO/IEC-27001:2014 en base a la información documentada del gobierno central del Perú?, (b) ¿ Cuál es el nivel de la percepción de la implementación de las cláusulas de ejecución de la NTP

ISO/IEC-27001:2014 en base a la información documentada del gobierno central del Perú? , (c) ¿Cuál es el nivel de la percepción de la implementación de las cláusulas de verificación de la NTP ISO/IEC-27001:2014 en base a la información documentada del gobierno central del Perú? y (d) ¿ Cuál es el nivel de la percepción de la implementación de las cláusulas de mejora continua de la NTP ISO/IEC-27001:2014 en base a la información documentada del gobierno central del Perú?.

En ese sentido, la investigación se justifica desde el punto de vista práctico porque trae a colación la relevancia de implementar el Sistema de Gestión de Seguridad de la Información en las entidades del Gobierno Central de Perú, proporcionando una referencia para el inicio, mantenimiento o mejora continua de la implementación de la NTP-ISO/IEC 27001:2014 en las entidades públicas; asimismo, metodológicamente, aportará un instrumento a otras entidades del estado, permitiéndoles identificar la documentación del marco regulatorio peruano, entre ellos, los instrumentos de gestión tales como el Plan Estratégico Institucional - PEI, Plan Operativo Institucional - POI, Reglamento de Organización y Funciones - ROF, Manual de Procedimientos – MAPRO, Plan de Desarrollo de Personas - PDP, Plan Anual de Contrataciones - PAC, así como el Portal de Transparencia estándar- PTE, Plataforma Digital Única del estado peruano ".gob.pe", Lineamientos del Comité de Gobierno Digital, entre otros; los cuales estarán alineados a los requisitos documentales de la NTP ISO/IEC 27001:2014. Por otra parte, teóricamente se justifica porque a través del estudio de puntos de vista diferentes en diversas investigaciones permitirá tener el debido sustento técnico, permitiendo a futuras investigaciones y/o entidades públicas del estado peruano tener una fuente para iniciar con la información documentada que especifica la NTP ISO/IEC 27001:2014. Y finalmente, desde el punto de vista político se justifica, considerando que, el gobierno del Perú a través de la Presidencia de Consejo de Ministros – PCM, ha formulado la propuesta de la Política Nacional de Transformación Digital estando a puertas de su aprobación, con lo cual la presente respalda el aporte de la academia al marco de confianza digital.

El objetivo propuesto en la investigación fue: Determinar el nivel de la

percepción de la implementación de la NTP ISO/IEC-27001:2014 en base a la información documentada del poder ejecutivo en el nivel de gobierno central del Perú. Y, como objetivos específicos: (a) Determinar el nivel de la percepción de la implementación de las cláusulas de planificación de la NTP ISO/IEC-27001:2014 en base a la información documentada del poder ejecutivo en el nivel de gobierno central del Perú, (b) Determinar el nivel de la percepción de la implementación de las cláusulas de ejecución de la NTP ISO/IEC-27001:2014 en base a la información documentada del poder ejecutivo en el nivel de gobierno central, (c) Determinar el nivel de la percepción de la implementación de las cláusulas de verificación de la NTP ISO/IEC-27001:2014 en base a la información documentada del poder ejecutivo en el nivel de gobierno central del Perú y (d) Determinar el nivel de la percepción de la implementación de las cláusulas de mejora continua de la NTP ISO/IEC-27001:2014 en base a la información documentada del poder ejecutivo en el nivel de gobierno central del Perú.

II. MARCO TEÓRICO

En referencia a los trabajos previos revisados en el contexto internacional sobre la seguridad de la información, se tiene a Najar y Suarez (2015) quienes señalan que, la información se encuentra altamente expuesto por depender tanto de factores internos como externos; ellos concluyen, que la información, al ser considerado como uno de los activos más importante, debe tenerse un cuidado y protección especial, dado que al no tenerlos son aprovechados por cibercriminales que operan a nivel internacional, afectando a todo tipo de sectores tanto en el ámbito público como privado.

En esa línea, Najar (2016) en dicha investigación aborda de manera amplia y detallada las formas y niveles a la que se encuentra expuesta la información de las organizaciones, concluyendo que el activo más valioso de las organizaciones siempre se encontrará expuesto, situación que debe aceptarse en su justa medida apostando por la investigación, desarrollo y

capacitación; de la misma manera Rivera Guerrero et al. (2019) , concluyen que en la actualidad la información se ha transformado en un activo intangible que requiere de garantizar su integridad, su disponibilidad y confidencialidad.

Frente a lo descrito en el párrafo anterior, la Organización Internacional para la Normalización - ISO y la Comisión Electrotécnica Internacional - IEC crean la norma ISO/IEC 27001:2013 sobre las TI y las técnicas de seguridad denominada “Sistemas de gestión de seguridad de la información - SGSI. Requisitos”; la cual establece que un SGSI o ISMS por su definición en inglés Information Security Management System (ISO y IEC, 2013), es el sistema que “preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente”, expresada en la versión traducida al idioma español para el Perú (Indecopi, 2014). Así también, lo explica Humphreys (2016), indicando que la norma internacional ISO/IEC 27001 es un conjunto de requisitos para establecer, implementar, monitorear, revisar, mantener, actualizar y mejorar un SGSI documentado con respecto a los riesgos y oportunidades comerciales generales de la organización.

En esa línea, considerando que la norma ISO/IEC 27001 buscar mantener un SGSI documentado, es preciso mencionar a Kosutic (2017), quien señala que la información documentada mencionada en la norma ISO, se refiere a los documentos y registros del SGSI; y que éstos se constituyen en la herramienta para mejorar de la seguridad de la información en una organización; menciona también, en relación a la información documentada, que ésta, ayuda a los empleados a realizar mejor sus actividades y procesos, evitando que éstos se vuelvan incontrolables. Para ello toda organización debe identificar la documentación necesaria que conformará su SGSI a fin de que esté se cumpla con los requisitos ISO 27001 (Vergara, 2019).

Franch y Guerra Bretaña (2016), en su propuesta sobre un modelo que integra la gestión del conocimiento operativo y el control de la información documentada en la investigación universitaria, resalta el hecho de que en cierta medida, el conocimiento producido dentro de la organización es mantenido y conservado como información documentada.

Por otra parte, Chaparro (2016), en la elaboración de un plan de implementación de la ISO/IEC 27001:2013, indica que todos los sistemas de gestión están soportados en un cuerpo documental que están establecidos en la propia norma ISO/IEC 2700, y que de acuerdo a la serie de documentos que se plantean, resalta siete: Política de Seguridad, Procedimiento de Auditorías Internas, Gestión de Indicadores, Procedimiento Revisión por Dirección, Gestión de Roles y Responsabilidades, Metodología de Análisis de Riesgos y la Declaración de Aplicabilidad.

Eito-Brun y Calleja (2020) en su publicación acerca de la gestión documental en los modelos de gobernanza TIC, hace referencia que de acuerdo a la terminología usada en el conjunto de normas ISO 9001, ISO 14001 o ISO 27000, denominados sistemas de gestión integrados, indica que solo mediante una planificación y control efectivo de su información documentada y de las tecnologías, las organizaciones pueden demostrar su trayectoria y evidenciar de manera fehaciente la ejecución de sus actividades.

Gómez (2020), indica que un SGSI debe implementarse con la debida sistematización, documentación y debe ser conocido en toda la organización; indicando también que es posible trasladar el modelo de documentación de la ISO 9001 a la ISO 27001, por lo que los documentos y registros que se generen a partir del SGSI pertenecerán a cualquier de los cuatro niveles: en el Nivel 1, el Manual de Seguridad, en el Nivel 2 se encuentran los procedimientos, en el Nivel 3, conformado por las instrucciones y en el Nivel 4, se encuentran los registros, que vienen a ser la evidencia documentada de la información en el cumplimiento de la gestión del SGSI. Asimismo, define a los siguientes documentos como los principales requeridos por la norma ISO/IEC 27001:2013: Alcance del SGSI, Política y objetivos de seguridad, Procedimientos y mecanismos de control, Enfoque de evaluación de riesgos, Informe de evaluación de riesgos, Plan de tratamiento de riesgos, Procedimientos documentados, Registros, Declaración de aplicabilidad.

Muñoz (2020), menciona indistintamente a los requisitos documentales de la norma ISO 9001 con otras normas, entre ellas la ISO 27001, indicando que el control de la información documentada es el referido a su disponibilidad, garantizando su integridad y confidencialidad.

Continuando con el desarrollo de la precitada norma, Carvalho y Marques (2019), indican que los requisitos para el cumplimiento de la ISO/IEC 27001:2013 se encuentran desde la cuarta hasta la décima cláusula; como también lo consideran Shojaie, Federrath y Saberi (2014) en la evaluación que realizaron a la ISO 27001:2013, mencionan que los requisitos ineludibles en relación al establecimiento, implementación, mantenimiento y la mejora continua en un SGSI basado en el estándar en estudio, se encuentran definidos desde la cláusula 4 a la cláusula 10; también indican que éstas, han sido redactadas de tal manera que dejan abierta la posibilidad de emplear diferentes formas para su implementación y en orden indistinto a la correlatividad de la numeración de las cláusulas; por lo que podemos apreciar que las entidades públicas, quienes se rigen a cumplimientos normativos, así como, las empresas privadas de todos los sectores y de diferentes tamaños y de niveles de madurez pueden dar cumplimiento a la ISO/IEC 27001:2013; en ese sentido, para fines de la presente investigación utilizaremos el término "cláusulas" para referirnos los requisitos de la precitada norma.

Abordando el desarrollo del SGSI podemos citar a Valencia y Orozco (2017), quienes consideran que dentro de la fase diseño de un SGSI basado en la ISO/IEC 27001:2013, se debe considerar tres componentes, refiriéndose en primer lugar a la documentación o información documentada del sistema; precisando que ésta, irá surgiendo a medida que se vaya implementando cada una de las diferentes fases del SGSI. Asimismo, el BSI Group México (2013), indica que los requisitos y documentación que establece el estándar ISO 27001:2013, está distribuida por toda la norma y asciende a un total de dieciséis (16) ítems de información documentada, los cuales se detallan en el Anexo N° 06.

Por su parte, Carvajal et al. (2019) en la investigación que propone el diseño de un Sistema de Gestión de Seguridad de la Información, desarrolla tres fases, siendo la primera de ellas la Documentación del sistema, la cual se realiza en base a los requisitos de la ISO/IEC 27001:2013, citando el resumen de la Información Documentada que debe tener un SGSI basado en la ISO/IEC 27001:2013 elaborado por Valencia y Orozco, el cual se plasma en el Anexo N° 06, sobre ello, se puede apreciar, que a diferencia del análisis

realizado por el BSI Group México, tiene una ítem de documentación adicional, además y añade sustentos citando a los textos extraídos de la norma ISO/IEC 27001:2013.

Por otra parte, Berrio et al. (2016) sostiene que la norma ISO 27001 es un estándar con requisitos y de controles de seguridad con el fin de planificar, hacer, verificar y actuar en un SGSI, basado en el modelo de Deming; de manera similar, Mahecha y Coello (2016) en el desarrollo de un sistema para gestionar un SGSI, nos indican que la norma ISO 27001 trabaja bajo un enfoque a procesos que ayuda a establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente el SGSI de las organizaciones, incluyéndose el empleo del ciclo Deming, ello, en el marco de tener buenas prácticas de mejora continua, empezando por la etapa de planear, en la cual se establece el SGSI definiendo su alcance, luego en la etapa de hacer, que es la etapa en la que se implementa y opera el SGSI, continua con la etapa de verificar en la que se identifican brechas entre lo planificado y lo ejecutado por el SGSI y finaliza con la etapa de actuar, en donde se aplican cambios en la ejecución del SGSI para lo cual se debe volver a planificar y reiniciar el ciclo del SGSI; cabe precisar que dicho ciclo de mejora continua conforme a lo precisado por Pérez(2012), es un ciclo dinámico que puede implementarse en la organización como un todo o dentro de cada proceso de manera individual.

Por otra parte, Cuatrecasas (2010), define al ciclo Deming como la herramienta que permitirá lograr la mejora continua de una forma sistemática y estructurada: definiendo cuatro fases que se realizan en un ciclo repetitivo: Planear, Realizar, Verificar y Actuar, también conocido como ciclo PDCA, siglas en inglés de Plan, Do, Check, Act, ayudando de esta manera a emplear la lógica y comprender la importancia de estas fases.

Rodríguez (2017), en su tesis sobre el Diseño de un SGSI, lo explica de manera más resumida indicando que el ciclo PDCA, permite Planear(plan), etapa en donde se definen metas y los mecanismos de cómo serán alcanzadas, Hacer(do), etapa que después de haber realizado un proceso de formación se ejecutan y recogen todos los datos, Verificar(check), etapa en la cual se evalúan los resultados e identifican los problemas no resueltos y la

etapa Actuar(act), en la cual se formulan y ejecutan planes con las medidas correctivas que lograrían el cumplimiento de las metas.

De manera similar, Rodríguez y Umenza (2018), indica los objetivos y definición de las etapas de “Planificar” “Hacer” “Verificar” “Actuar”, siendo el objetivo de “Planificar”, el establecimiento del SGSI, creando la política, los objetivos, procesos y procedimientos de seguridad que sean considerados pertinentes en el marco de gestionar los riesgos y mejorar la seguridad de la información con la finalidad de lograr resultados según las políticas y objetivos de la alta dirección de las organizaciones. La etapa “Hacer”, tiene como objetivo la de “Implementar y operar el SGSI”, poniendo en práctica la política, los controles, procesos y procedimientos del SGSI. La etapa de “Verificar”, es la que corresponde al seguimiento y revisión del SGSI, en la cual se mide la el desempeño de los procesos en relación con la política, los objetivos de seguridad y la experiencia práctica y reportar los resultados a la dirección para su revisión; y la etapa final del ciclo de mejora continua, “Actuar”, corresponde al mantenimiento y mejora del SGSI; en la cual se emprenden las acciones correctivas y preventivas con base en los resultados de la auditoría interna y la revisión por la dirección.

De manera similar, García et al. (2003), describen a la etapa de “Planificar”, como la etapa de establecer objetivos y definir los procesos necesarios para obtener los resultados en conformidad con los requisitos del cliente y las políticas de la organización a través de herramientas; la etapa “Hacer”, la definen como aquella en donde se ejecutan los procesos para lograr los objetivos. En cuanto a la etapa de “Verificar”, indican que es aquella en donde se realiza el seguimiento a través de la medición de los productos de procesos y su relación la política, objetivos y requisitos, con los resultados alcanzados; proveyendo de indicadores que permitan tener una lectura de lo llevado a cabo a fin de que favorezca el seguimiento de los procesos; y finalizan indicando que la etapa “Actuar”, es aquella en donde se realizan acciones para promover la mejora continua del desempeño del (los) proceso(s).

Retomando de los antecedentes teóricos de acerca de la ISO 27001, Rodríguez y Umenza(2018), en su publicación ilustran las cláusulas de la

norma y su aplicación por cada fase del ciclo Demming, indicándonos que para la etapa de Planificación(planear) considera a las cláusulas de Contexto de la Organización, Liderazgo, Planeación y la de Soporte, en la etapa de Ejecución(hacer) considera la cláusula de Operación, en la etapa de Verificación (verificar) considera la cláusula Evaluación de Desempeño y la etapa de Mejora Continua(actuar) tiene la cláusula décima denominada Mejora Continua.

Asimismo, Bayona et al. (2015), en su investigación de implementación de la ISO/IEC 27001 en entidades públicas, precisan factores críticos para la implementación de un SGSI extraído de ocho autores diferentes; en donde, si bien uno de dichos autores, considera a la documentación como un factor crítico dentro de la categoría Desarrollo de controles de Seguridad; se puede observar en su informe que existen diversos factores críticos que necesariamente deben ser documentados, por citar algunos, la Misión de la Organización, la Estructura organizacional, las Políticas, la Evaluación del desempeño, entre otros. Asimismo, abordan el caso de dos empresas del sector público, donde se aprecia que los criterios asociados a las cláusulas de planificación y ejecución son percibidos como factores de éxito en un 68% para la implementación del SGSI y con respecto a las cláusulas de verificación las perciben como factor de éxito en un 56%.

Asimismo, Benitez (2016), tiene una percepción acerca de que, en las implementaciones en las organizaciones de un SGSI, la etapa de la planificación es la más desventajosa, dado que la norma ISO 27001 es descrita de una manera muy general y considerando las grandes diferencias entre distintas organizaciones, esto puede impactar la efectividad de su implementación.

Finalmente, en base al diagnóstico realizado en dos investigaciones en una entidad del estado peruano y en una privada de Colombia realizado por Vásquez (2018) y Viveros (2017) respectivamente, podemos apreciar que acuerdo al diagnóstico del nivel de madurez presentado en sus investigaciones que se cuenta con una implementación en promedio de 68% de las cláusulas de planificación, 50% de las cláusulas de ejecución, 75% de las cláusulas de verificación y 58% de las cláusulas de mejora continua.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Para este estudio se ha considerado el tipo de investigación aplicada, que según Sánchez (1998) la llama utilitaria y la define como el tipo de investigación que se centra en aplicar conocimientos teóricos a una situación específica y las consecuencias prácticas que generen; y que según Noguera (2003) la denomina práctica dado que está dirigida a la acción sobre la realidad objeto de estudio; en ese sentido, en esta investigación se estarán abordando las teorías sobre la ISO/IEC 27001:2013 y su información documentada aplicadas a la gestión de la seguridad de la información en las entidades del poder ejecutivo del gobierno central.

El diseño de investigación corresponde al descriptivo simple, que de acuerdo con Hernández et al. (2014), definen a este diseño como “aquellos que indagan las incidencias de las modalidades, categorías o niveles de una o más variables en una población”. Asimismo, también la podemos clasificar como una investigación no experimental, que de acuerdo con Hernández y Mendoza (2018), es un estudio sin realizar variaciones o manipulaciones en las variables en su contexto natural; considerando que la finalidad de esta investigación es recoger datos del Diagnóstico de las cláusulas de la información documentada en la implementación de la NTP-ISO/IEC-27001:2014, para describir su estado. También se denomina transeccional porque se recogerá la información en una sola oportunidad. Este diseño presenta el siguiente esquema:

M O

Dónde:

M : Servidores públicos relacionados con la gestión de las TI y seguridad de la información e informática.

O : Percepción de la implementación de la NTP ISO/IEC 27001:2014 en base a la información documentada

3.2. Variables y operacionalización

Para definir conceptualmente la variable Percepción de la implementación de la NTP-ISO/IEC-27001:2014 en base a la información documentada, se ha integrado una serie de referencias, definiéndose como, el recojo de nivel de implementación de la implementación de la NTP-ISO/IEC-27001:2014 en base a los requisitos de las cláusulas relacionadas a la información documentada y por los determinados y/o en uso por las entidades que conforman el Gobierno Central en la implementación de sus Sistema de Gestión de Seguridad de la Información.

Asimismo, operacionalmente, la variable es el recojo de la percepción sobre la implementación de la NTP ISO/IEC 27001:2014 de la cláusula de Planificación, en la que se establece y define el alcance del SGSI, de Ejecución, en la que se opera el SGSI, de Verificación, en la que se identifican brechas entre lo planificado y lo ejecutado y de mejora continua, en la que se aplican cambios en la ejecución para volver a planificar y reiniciar el ciclo del SGSI, por medio de la técnica de la encuesta y de un cuestionario de preguntas cerradas. Mahecha y Coello (2016)

Por lo expuesto y considerando los puntos de vista expuestos en el marco teórico, se han considerado fases del ciclo Deming PHVA y los requisitos documentales de las cláusulas de la norma ISO/IEC 27001:2013 que para fines de esta investigación serán tomados como dimensiones e indicadores respectivamente.

3.3. Población, muestra, muestreo, unidad de análisis

La población, de acuerdo a lo indicado por García (2016), es “un conjunto de personas, objetos, cosas u otra característica común y que ocupan o desempeñan un espacio o contexto de trabajo determinado”, de manera similar, Hernández et al. (2014) lo señala como las concordancias de una serie de especificaciones; resumiendo ello, es preciso citar a Valderrama (2015), quien señala que es el conjunto de individuos con características similares; en ese sentido, para esta investigación nuestra población está conformada por

setenta y seis(N=76) servidores públicos relacionados con la gestión de las TI y seguridad de la información e informática pertenecientes a los 19 sectores del poder ejecutivo del Perú en el nivel de gobierno central, tal como se muestra a continuación:

Tabla 1

Población de la Percepción de la implementación de la NTP ISO/IEC 27001:2014 en base a la información documentada

N°	Sector	Cantidad Personas (*)
1	Agricultura	4
2	Ambiente	4
3	Comercio Exterior y Turismo	4
4	Cultura	4
5	Defensa	4
6	Desarrollo e Inclusión Social	4
7	Economía y Finanzas	4
8	Educación	4
9	Energía y Minas	4
10	Interior	4
11	Justicia	4
12	Mujer y Poblaciones Vulnerables	4
13	Presidencia del Consejo de Ministros	4
14	Producción	4
15	Relaciones Exteriores	4
16	Salud	4
17	Trabajo y Promoción del Empleo	4
18	Transportes y Comunicaciones	4
19	Vivienda, Construcción y Saneamiento	4
	Total	76

Nota: Se considera cuatro personas por cada sector: un director o jefe de TI, un supervisor o coordinador de TI, un profesional en seguridad informática y el/la Oficial de Seguridad de la Información.

Asimismo, considerando que la cantidad de las unidades de análisis que conforman la población es una cantidad alcanzable para el recojo de la información, se ha creído conveniente que la muestra debe tener el mismo tamaño que la población (N=n=76), correspondiendo a una muestra censal, definido por Hayes (1999) como aquella en donde “la cantidad de la muestra

es igual a la población, esta clasificación se utiliza cuando la población en relativamente pequeño" (p. 56). Por lo que en el presente estudio se considera un muestreo no probabilístico e intencional, dado que, de acuerdo con lo señalado por Arias (2006) indica que el muestreo puede ser intencional u opinático cuando la muestra es escogida teniendo como base a los criterios preestablecidos del investigador; siendo este el caso de la presente investigación, dado que la selección estuvo sujeto a la accesibilidad y competencias para proporcionar la información materia de estudio, y en añadidura a ello, se tiene falta de accesibilidad a los encuestados al no poderse establecer comunicaciones agiles por el trabajo remoto que se viene ejerciendo en la coyuntura actual por la pandemia del COVID-19; no considerándose a los servidores que no se tienen facilidades de comunicación.

3.4. Técnicas e instrumentos de recolección de datos

Considerando que la encuesta es un método para la recolección de información y que según Alvira (2011, p.6) indica que la información que se recoge puede ser escrita mediante un cuestionario estructurado, en este estudio se ha empleado la técnica de la encuesta por su versatilidad para recoger los datos de una variable.

Con respecto al instrumento, se empleará un cuestionario de preguntas cerradas, las cuales según Bernal (2010) son aquellas preguntas en donde la respuesta solicitada contiene una lista de opciones; dichas respuestas están dadas en una escala de medición ordinal, que de acuerdo con Gómez (2012) quien sostiene que ese tipo de escala "se jerarquizan considerando un rango, para lograr establecer una gradación entre uno y otro valor de la escala" (p.67).En ese sentido, para el presente estudio, se tiene la escala ordinal de cinco alternativas (1 - Muy Poco, 2 – Poco, 3 – Regular, 4 – Mucho, 5 – Muchísimo).

Asimismo, Este instrumento consta de cuarenta ítems o reactivos distribuidos en cuatro dimensiones (Planificación con 28 ítems, Ejecución con

4 ítems, Verificación con 4 ítems y Mejora Continua con 4 ítems).

La validez de un instrumento de investigación, según Hernández et al. (2014) indica que se refiere “al grado en que un instrumento mide realmente la variable que pretende medir” (p. 200); en ese sentido, en esta investigación se consideró una validación a criterio del juicio de expertos, con un total de tres expertos, siendo uno de ellos, el docente principal de la asignatura y dos expertos externos, con grados de doctor y de magister, éste último con especialidad en la materia de estudio.

Tabla 2

Validación de Juicio de Expertos

N°	Experto	Especialidad	Aplicable
Experto 1	Dr. Alejandro Ramírez Ríos	Ciencias de la Educación	Si
Experto 2	Mg. Elvis Gonzalo Malpartida Asencio	Ingeniería de Sistemas	Si
Experto 3	Dr. Nicolas Álvarez Carrillo	Matemática, Física	Si

Con respecto a la confiabilidad del instrumento de medición, Hernández et al. (2014) menciona que es el “grado en que su aplicación repetida al mismo individuo u objeto produce resultados iguales” (p.200).; para el caso de estudio, se determinó a través de la prueba estadística Alfa de Cronbach, cuyo valor obtenido $\alpha_{crombach} = 0{,}991$, tal como lo establece Valderrama (2015), quien menciona también, que la confiabilidad oscila desde 0 hasta 1, representando una confiabilidad nula o total respectivamente.

En ese sentido, la confiabilidad del instrumento de esta investigación se encuentra cercano al valor 1, por lo que se ha calificado como un instrumento de alta confiabilidad, por lo que resulto ser aplicable; dicho valor pudo ser obtenido al procesar la muestra piloto de n=20, tal como se puede visualizar en el Anexo 5.

Tabla 3

Fiabilidad de la variable NTP ISO/IEC 27001:2014

Alfa de Cronbach	N° de ítems
0.991	40

3.5. Procedimientos

Primero se construyó el instrumento a partir de la matriz de operativización de la variable; luego de ello, se determinó la validez y la confiabilidad del instrumento; se aplicó el cuestionario de preguntas cerradas a la muestra censal; se procesaron los datos en la solución de software estadístico; se presentaron los resultados de acuerdo con los objetivos planteados al inicio de la investigación; se realizó la discusión de los datos y se obtuvo las conclusiones; y, finalmente se elaboraron las recomendaciones.

3.6. Método de análisis de datos

Para analizar los datos se utilizó la estadística descriptiva simple, se analizó, interpretó y concluyo en base a los resultados. La estadística por utilizar es de tablas de frecuencias y figuras de diagramas de barras (tablas y gráficos de variables cualitativas). Asimismo, en cuanto a la información recogida, ésta será procesada con el software de soluciones estadísticas SPSS.

3.7. Aspectos éticos

La información recogida es consentida por la Presidencia del Consejo de Ministros y los diversos jefes de las dependencias de tecnologías de información que constituyen la muestra en estudio, y será utilizada solamente para los fines de la investigación; asimismo, la administración de los cuestionarios es anónima. Por otro lado, la información recogida que fundamenta la investigación es obtenida directamente de la fuente para dar legitimidad al estudio y ser aprobado por el turnitin.

Se ha desarrollado en base a la guía de elaboración del trabajo de investigación y tesis para la obtención de los grados académicos y títulos profesionales de la Universidad Cesar Vallejo aprobada con Resolución de Vicerrectorado de Investigación N° 011-2020-VI-UCV.

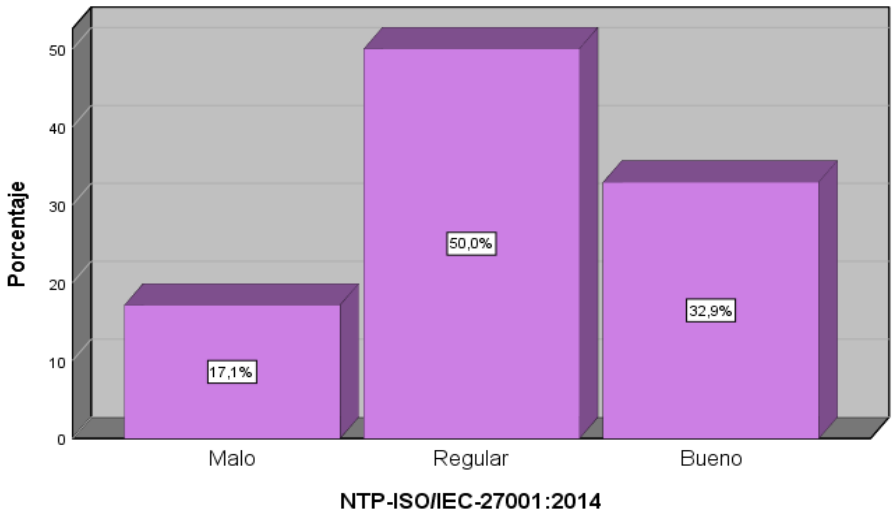
IV. RESULTADOS

A continuación, se detallan las frecuencias y porcentajes de la percepción de la variable NTP-ISO/IEC-27001:2014 y de sus dimensiones de planificación, ejecución, verificación y mejora continua:

Tabla 4
Frecuencia y porcentaje de los niveles de la variable NTP ISO/IEC27001:2014

		Frecuencia	Porcentaje
Válido	Malo	13	17,1%
	Regular	38	50%
	Bueno	25	32,9%
	Total	76	100%

Figura 1
Percepción de la NTP ISO/IEC 27001:2014.



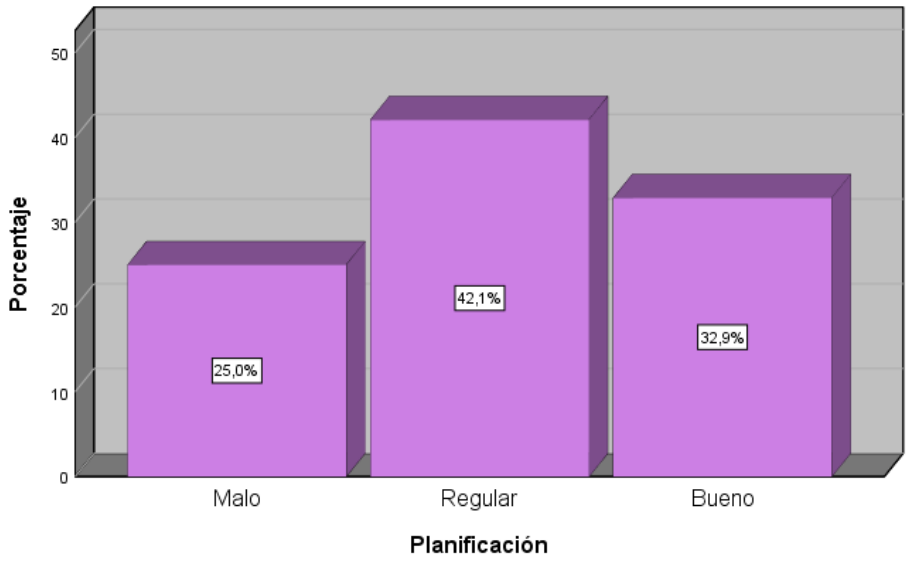
De acuerdo con los resultados presentados, se muestra que el 50% de los encuestados perciben que la implementación de la NTP ISO/IEC 27001:2014 en base a la información documentada del gobierno central del Perú, es regular, el 32.9% de los encuestados opinan que es bueno y el 17.1% de los encuestados señalan que es malo. Es decir, que el SGSI implementado en las entidades de los encuestados no perciben que las cláusulas de la NTP

ISO/IEC 27001:2014 están cumpliendo para el fin que fueron creadas, o en su defecto desconocen su implementación en su entidad o no se cuenta con la información documentada acerca de la implementación de la NTP ISO/IEC 27001:2014.

Tabla 5
Frecuencia y porcentaje de los niveles de la dimensión planificación

		Frecuencia	Porcentaje
Válido	Malo	19	25,0%
	Regular	32	42,1%
	Bueno	25	32,9%
	Total	76	100%

Figura 2
Percepción de la planificación.



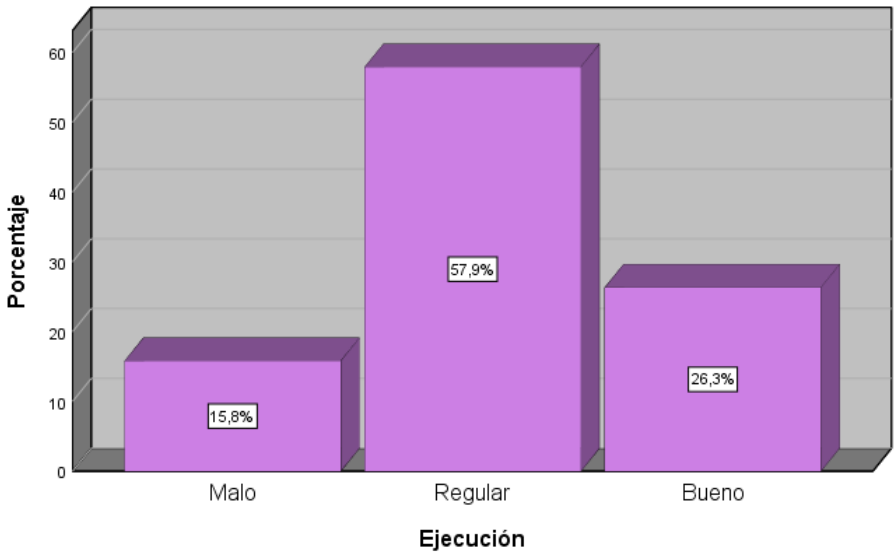
Con respecto a los resultados de la primera dimensión, se muestra que el 42.1% de los encuestados perciben que la planificación es regular, el 32.9% de los encuestados la perciben como bueno y el 25% de los encuestados la perciben como mala. Es decir, que perciben que la implementación de las cláusulas de planificación de la NTP ISO/IEC 27001:2014 en sus respectivas entidades, tienen un nivel regular con respecto al propósito para el que fueron creadas, o no han sido implementadas, o no cuentan con información

documentada o en su defecto la información documentada de las cláusulas de planificación, tales como, el alcance, política de seguridad, roles y responsabilidades; valoración y tratamiento de riesgos, objetivos de seguridad de la información; de la gestión de los recursos, de la gestión de las competencias, de la gestión de la concientización, de la gestión de la comunicación y la de los documentos y registros, han sido parcialmente comunicados y/o distribuidos.

Tabla 6
Frecuencia y porcentaje de los niveles de la dimensión ejecución

		Frecuencia	Porcentaje
Válido	Malo	12	15,8%
	Regular	44	57,9%
	Bueno	20	26,3%
	Total	76	100%

Figura 3
Percepción de la ejecución.



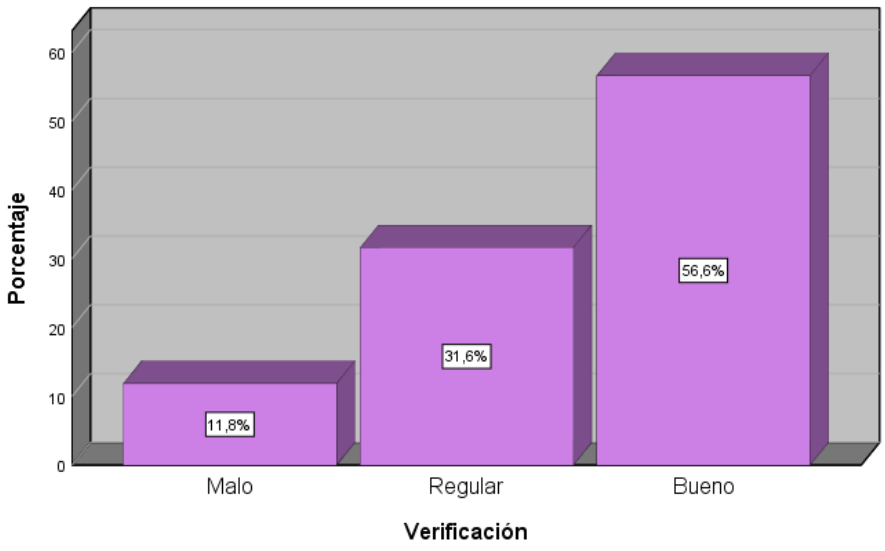
Con respecto a los resultados de la segunda dimensión, se muestra que el 57.9% de los encuestados perciben que la ejecución es regular, el 26.3% de los encuestados la perciben como bueno y el 15.8% de los encuestados la perciben como mala. Es decir, que perciben que la implementación de las

cláusulas de ejecución de la NTP ISO/IEC 27001:2014 en sus respectivas entidades, tienen un nivel regular con respecto al propósito para el que fueron creadas, o no han sido implementadas, o no cuentan con información documentada o en su defecto la información documentada de las cláusulas de mejora continua, tales como, el POI con tareas relacionadas al SGSI, gestión de riesgos con las nuevas amenazas, vulnerabilidades y riesgos de seguridad de la información producto de la operatividad diaria del SGSI, han sido parcialmente comunicados y/o distribuidos.

Tabla 7
Frecuencia y porcentaje de los niveles de la dimensión verificación

		Frecuencia	Porcentaje
Válido	Malo	9	11,8%
	Regular	24	31,6%
	Bueno	43	56,6%
	Total	76	100%

Figura 4
Percepción de la verificación.



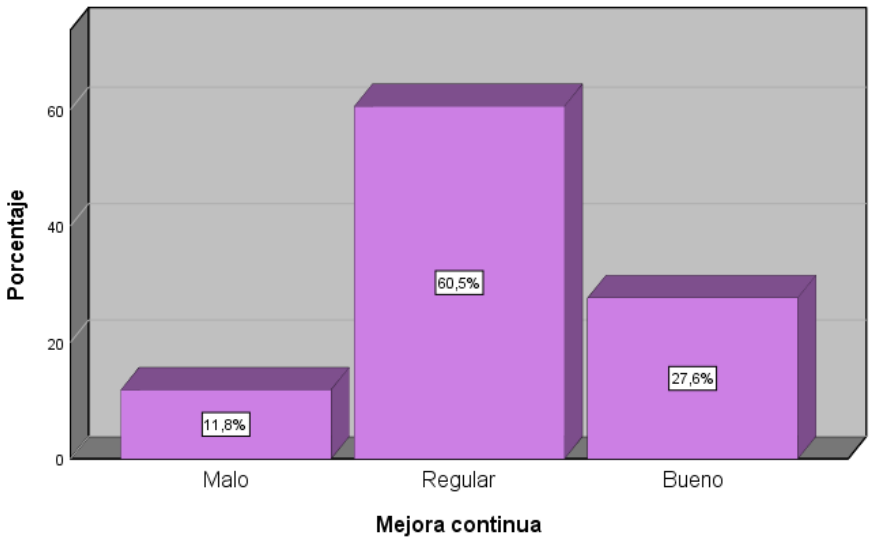
Con respecto a los resultados de la tercera dimensión, se muestra que el 56.6% de los encuestados perciben que la verificación tiene un nivel bueno,

el 31.6% de los encuestados la perciben como regular y el 11.8% de los encuestados la perciben como mala. Es decir, que perciben que la implementación de las cláusulas de verificación de la NTP ISO/IEC 27001:2014 en sus respectivas entidades, tienen un nivel bueno con respecto al propósito para el que fueron creadas y su información documentada, como los indicadores, metas y la medición del logro de los objetivos planteados en el SGSI, el procedimiento y/o programa de auditorías internas, los hallazgos de las auditorías internas, los informes de progreso del SGSI suscritos por el Comité de Gobierno Digital han sido debidamente comunicados y/o distribuidos.

Tabla 8
Frecuencia y porcentaje de los niveles de la dimensión mejora continua

		Frecuencia	Porcentaje
Válido	Malo	9	11,8%
	Regular	46	60,5%
	Bueno	21	27,6%
	Total	76	100%

Figura 5
Percepción de la mejora continua.



Con respecto a los resultados de la cuarta dimensión, se muestra que el

60.5% de los encuestados perciben que la mejora continua es regular, el 27.6% de los encuestados la perciben como bueno y el 11.8% de los encuestados la perciben como mala. Es decir, que perciben que la implementación de las cláusulas de mejora continua de la NTP ISO/IEC 27001:2014 en sus respectivas entidades, tienen un nivel regular con respecto al propósito para el que fueron creadas, o no han sido implementadas, o no cuentan con información documentada o en su defecto la información documentada de las cláusulas de mejora continua, tales como, los incumplimientos de la NTP ISO/IEC 27001:2014, los planes de acción y acciones correctivas que subsanar los incumplimientos, y los informes frecuentes de acciones de mejora continua, han sido parcialmente comunicados y/o distribuidos.

V. DISCUSIÓN

Con respecto al objetivo general de determinar la percepción de la implementación de la NTP ISO/IEC-27001:2014, se puede apreciar que en términos generales, ésta se percibe como regular, dado que el 50% de los encuestados así lo expresaron; esto puede significar un balance entre la percepción de la necesidad de la implementación de la NTP ISO/IEC-27001:2014 y la forma en como la información documentada se viene elaborando y/o gestionando; ampliando ello, en relación a la necesidad de su implementación, lo cual es producto de que los encuestados perciben que el SGSI atiende las necesidades de seguridad de la información de los procesos misionales, los procesos estratégicos y los servicios brindados a la ciudadanía, conforme a lo identificado en el tercer y cuarto ítem del primer indicador del instrumento de la investigación denominado Alcance del SGSI, en el cual se obtuvo en promedio la valoración mucho, esto es, por percibir que los activos de información son de un muy alto valor y críticos para las operaciones diarias de sus respectivas entidades.

En esa línea, se puede apreciar que lo precitado concuerda con lo indicado, en primer lugar por Najar y Suarez (2015), al señalar que la

información por ser el activo más importante de las organizaciones, debe tenerse un especial cuidado y protección; en esa misma línea, concuerda también con lo mencionado en la publicación individual de Najar (2016), en la que concluyó que la exposición del activo más valioso de las organizaciones debe aceptarse en su justa medida apostando por la investigación, desarrollo y capacitación; así también lo señalaron Rivera Guerrero et al. (2019), quienes indicaron que en la actualidad, la información se ha transformado en un activo intangible que requiere de garantizar su integridad, su disponibilidad y confidencialidad, pilares de la seguridad de la información.

Continuando con ello, referente a la forma en como la información documentada se viene elaborando y/o gestionando, es producto de que los encuestados perciben que los documentos determinados y el procedimiento para su gestión están contribuyendo a gestionar de manera regular la seguridad de la información de sus entidades, esto, conforme a lo identificado en las respuestas del décimo al treceavo indicador del instrumento de la investigación, en el cual se obtuvo en promedio una valoración regular. Esto puede deberse a que no se han identificado o relacionado las cláusulas con la documentación empleada en sus actividades diarias o no están realizándola de manera previa a sus actividades, desvirtuando el propósito de la información documentada, no cumpliéndose lo fundamentado por Kosutic (2017), quien indica que la información documentada debe ayudar a los empleados a realizar mejor sus actividades y procesos, a fin de evitar que éstos se vuelvan incontrolables; o también podría deberse a que los implementadores del SGSI encuestados no han identificado de manera óptima la documentación necesaria para sus SGSI, tal como lo manifiesta Vergara(2019).

Con respecto al objetivo específico de determinar la percepción de la implementación de las cláusulas de planificación de la NTP ISO/IEC-27001:2014, se puede apreciar que ésta, se percibe como regular, dado que el valor más alto asciende a 42.1% en virtud de lo expresado por los encuestados; ello debido a que han percibido que en un nivel regular el SGSI: 1) está alineado a la situación y/o marco normativo externo, 2) contribuye al

cumplimiento de los planes institucionales y normatividad interna, 3) atiende las necesidades de seguridad de la información de los procesos misionales, estratégicos y de los servicios a la ciudadanía; 4) gestiona las relaciones comerciales y/o de cooperación en un marco de confianza, 5) ha abarcado los procesos principales en el alcance, 6) genera compromiso con la seguridad de la información, 7) está alineado a las responsabilidades del Reglamento de organización y funciones – ROF, Plan Operativo Institucional - POI, comités internos, contratos, convenios, texto único de procedimientos administrativos – TUPA u otras responsabilidades internas y externas; 8) ayuda a afrontar el contexto actual, la adquisición de bienes y servicios, la suscripción de convenios, la asignación adecuada de recursos; 9) está relacionado a la gestión de recursos humanos, como la definición de perfiles de puestos, el Plan de Desarrollo de Personas, los legajos de personal, la inducción al personal y la guías para usuarios finales; 10) la gestión documental a nivel interno y externo, así la gestión de las comunicaciones en el Portal .Gob.pe y el portal de transparencia, conforme a lo planteado en las preguntas del cuestionario.

En ese sentido, Bayona et al. (2015), en su investigación sobre implementación de la ISO/IEC 27001 en entidades públicas del estado peruano, abordan dos casos, donde se percibe que los criterios asociados a las cláusulas de planificación son factores de éxito en un 68%, es decir que tienen una percepción buena en el éxito de la implementación de un SGSI según la NTP ISO/IEC-27001:2014 teniéndose una pequeña diferencia en relación a los resultados de esta investigación que la percibieron como regular.

Del mismo modo, la percepción de las cláusulas de planificación diverge con lo obtenido en dos estudios realizados a entidades de Perú y Colombia por Vásquez (2018) y Viveros (2017) respectivamente, en donde se puede apreciar que acuerdo al diagnóstico del nivel de madurez presentado en sus investigaciones se cuenta con una implementación en promedio de 68% de las cláusulas de planificación, siendo estas de un nivel bueno. Dicho esto, podemos afirmar que cuando se trata de medir la percepción de la implementación de las cláusulas de planificación no se evidencia lo señalado

por Benitez (2016), quien indica que la mayor desventaja de la norma es que al ser muy amplia puede divergir en las maneras de implementarlas en la etapa de planificación.

Con respecto al objetivo específico de determinar la percepción de la implementación de las cláusulas de ejecución de la NTP ISO/IEC-27001:2014, se puede apreciar que ésta, se percibe como regular, dado que el valor más alto asciende a 57.9% en virtud de lo expresado por los encuestados; ello debido a que han percibido que en un nivel regular el SGSI: 1) se relaciona con la formulación y seguimiento de las tareas del POI, 2) que la gestión de riesgos de la seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad, la suscripción de nuevos contratos, convenios o adendas; así como la medición de la efectividad de los contratos, convenios y planes ejecutados en sus entidades conforme a lo planteado en las preguntas del cuestionario.

En ese sentido, Bayona et al. (2015), en su investigación sobre implementación de la ISO/IEC 27001 en entidades públicas del estado peruano, abordan dos casos, donde se percibe que los criterios asociados a las cláusulas de ejecución son factores de éxito en un 68%, es decir que tienen una percepción buena en el éxito de la implementación de un SGSI según la NTP ISO/IEC-27001:2014 encontrándose una ligera diferencia con los resultados en esta investigación que la percibieron también como regular.

Por otra parte, existe similitud, con respecto a los resultados de los estudios realizados por Vásquez (2018) y Viveros (2017), en el cual se obtuvo una valoración del 50% con relación al diagnóstico del nivel de madurez asociado a la implementación de las cláusulas de ejecución, siendo estas de un nivel regular al igual que la percepción de esta investigación, al haber obtenido 57.9%.

Con respecto al objetivo específico de determinar la percepción de la implementación de las cláusulas de verificación de la NTP ISO/IEC-27001:2014, se puede apreciar que ésta, se percibe como buena, dado que el valor más alto asciende a 56.6% en virtud de lo expresado por los

encuestados; ello debido a que han percibido que en un nivel bueno el SGSI: 1) ha establecido indicadores, metas y mecanismos de medición del cumplimiento de los objetivos de seguridad de la información, 2) que las auditorías internas programadas y sus resultados documentados, y que 3) los informes de su progreso suscritos por el Comité de Gobierno Digital, han contribuido a mejorar la seguridad de la información de sus entidades, conforme a lo planteado en las preguntas del cuestionario.

En ese sentido, Bayona et al. (2015), en su investigación sobre implementación de la ISO/IEC 27001 en entidades públicas del estado peruano, abordan dos casos, donde se percibe que los criterios asociados a las cláusulas de verificación son factores de éxito en un 56%, es decir que tienen una percepción buena en el éxito de la implementación de un SGSI según la NTP ISO/IEC-27001:2014 coincidiendo con los resultados de esta investigación que la percibieron también como buena. Se puede apreciar también que la valoración de este estudio coincide con los resultados obtenidos en los estudios de Perú y Colombia por Vásquez (2018) y Viveros (2017) respectivamente, en donde se puede apreciar que acuerdo al diagnóstico del nivel de madurez presentado en sus investigaciones se cuenta con una implementación en promedio de 75% de las cláusulas de verificación, siendo estas de un nivel bueno.

Con respecto al objetivo específico de determinar la percepción de la implementación de las cláusulas de mejora continua de la NTP ISO/IEC-27001:2014, se puede apreciar que ésta, se percibe como regular, dado que el valor más alto asciende a 60.5% en virtud de lo expresado por los encuestados; ello debido a que han percibido que en un nivel regular en el SGSI de sus entidades: 1) la documentación del incumplimiento de los requisitos de la NTP ISO/IEC-27001:2014, 2) los planes de acción para corregir los incumplimientos, y 3) los informes frecuentes de las acciones de mejora continua, contribuyen a mejorar la seguridad de la información de sus entidades, conforme a lo planteado en las preguntas del cuestionario.

Del mismo modo, la percepción de las cláusulas de mejora continua se asemeja con lo obtenido en los precitados estudios realizados por Vásquez

(2018) y Viveros (2017), en donde se puede apreciar que acuerdo al diagnóstico del nivel de madurez presentado en sus investigaciones se cuenta con una implementación en promedio de 58% de las cláusulas de mejora continua, siendo éstas de un nivel regular.

Por otra parte, con respecto a las fortalezas y debilidades de la metodología utilizada, al haberse obtenido la medición de la única variables así como de 3 de 4 dimensiones con una percepción regular, puede deberse a que, al haberse elegido como encuestados a los profesionales, que en su mayoría conforman el grupo de responsables de la implementación de la NTP ISO/IEC-27001:2014, el instrumento pudo significarles una especie de medición de la calidad y/o productividad de su trabajo; o que expondrían las deficiencias de gestión de sus respectivas entidades; otra causa pudo haber sido que la información documentada no ha sido debidamente distribuida o comunicada y que dicho desconocimiento por parte de los encuestados, sin incluir a los oficiales de seguridad de la información, optaron en responder la mayoría de preguntas con una valoración de regular.

Finalmente, con respecto a la relevancia de la presente investigación en relación con el contexto científico social en el que se desarrolla, considerando que, de acuerdo con la ley de creación de las entidades públicas en el estado peruano, la misión y funciones conferidas a cada entidad son irrepetibles entre sí, y que en virtud de ello la administración pública le confiere a cada entidad la salvaguarda de la información que vienen gestionando en el ámbito de sus competencias, es relevante considerar el presente estudio, toda vez que permitirá a los encuestados, a los servidores públicos y a la academia en general, tener un referente para el inicio, mantenimiento y/o mejora continua de la implementación NTP-ISO/IEC 27001:2014 en entidades públicas del estado peruano al emplear el instrumento de esta investigación, perfeccionándolo con otras investigaciones científicas relacionadas a la implementación de la NTP-ISO/IEC 27001:2014 en entidades públicas del Perú.

VI. CONCLUSIONES

Primera:

De acuerdo con el objetivo general, se logró determinar el nivel de la percepción de la implementación de la NTP ISO/IEC-27001:2014 en base a la información documentada en las entidades del poder ejecutivo en el nivel de gobierno central del Perú; obteniéndose que el 50% de los encuestados perciben que la implementación de la NTP-ISO/IEC 27001:2014 es regular.

Segunda:

De acuerdo con el primer objetivo específico, se pudo determinar que el nivel de la percepción de la implementación de las cláusulas de planificación de la NTP ISO/IEC-27001:2014 en base a la información documentada es regular, dado que así lo calificaron el 42.1% de los encuestados.

Tercera:

De acuerdo con el segundo objetivo específico, se pudo identificar que el nivel de la percepción de la implementación de las cláusulas de ejecución de la NTP ISO/IEC-27001:2014 en base a la información documentada es regular, dado que así lo calificaron el 57.9% de los encuestados.

Cuarta:

De acuerdo con el tercer objetivo específico, se pudo identificar que el nivel de la percepción de la implementación de las cláusulas de verificación de la NTP ISO/IEC-27001:2014 en base a la información documentada es bueno, dado que así lo calificaron el 56.6% de los encuestados.

Quinta:

De acuerdo con el cuarto objetivo específico, se pudo identificar que el nivel de la percepción de la implementación de las cláusulas de mejora continua de la NTP ISO/IEC-27001:2014 en base a la información documentada es regular, dado que así lo calificaron el 60.5% de los encuestados.

VII. RECOMENDACIONES

Primera:

El/la secretario/a de Gestión Pública de la PCM debe incorporar a las normas de gestión pública la referenciación de los documentos de la NTP ISO/IEC 27001:2014 descritos en el instrumento de la presente investigación.

Segunda:

El/la secretario/a de Gobierno Digital de la PCM debe elaborar los lineamientos del numeral 9.3 del Decreto de Urgencia N° 006-2020 referenciando los instrumentos de gestión descritos en el instrumento de la presente investigación.

Tercera:

Los presidentes de los Comités de Gobierno Digital deben incluir en los informes anuales que miden el progreso de la implementación del SGSI (R. M. N° 087-2019-PCM, artículo 2°, literal f) evidencias de haber empleado instrumentos de gestión.

Cuarta:

El/la presidente ejecutivo de la Autoridad Nacional del Servicio Civil – SERVIR debe dar plazos para la realización de las charlas de inducción o la entrega de guías para el personal nuevo en la Guía para la Gestión del Proceso de Inducción (Resolución de Presidencia Ejecutiva N° 265-2017-SERVIR-PE).

Quinta:

La máxima autoridad administrativa de las entidades del Poder ejecutivo del gobierno central, deben considerar al SGSI dentro de las actividades y sesiones de las Comisiones de Planeamiento Estratégico (Resolución de Presidencia de Consejo Directivo N° 062-2017-CEPLAN/PCD).

REFERENCIAS

Arias, F. (2006). *El proyecto de Investigación. Introducción a la metodología científica*. 6° edición. Caracas: Editorial Episteme.

Banco Interamericano de Desarrollo - BID & Organización de los estados americanos – OEA. (2020). Reporte de Ciberseguridad 2020. *Ciberseguridad, riesgos, avances y el camino a seguir en américa latina y el caribe*. https://bit.ly/3o4JcXN

Bayona, S., Chauca, W., Lopez, M. y Maldonado, C. (2015). *ISO/IEC 27001 implementation in public organizations: A case study*. 10th Iberian Conference on Information Systems and Technologies. Portugal. https://bit.ly/395SXk3

Benitez, D. (2016). *Revisión bibliográfica de la norma ISO 27001 y sus componentes*. (Trabajo de grado). Universidad Santo Tomas, Colombia. https://bit.ly/2Y5J9A8

Bernal, C. (2010). *Metodología de la investigación. administración, economía, humanidades y ciencias sociales*. 3° edición. Colombia: Editorial Pearson.

Berrío, J., Montoya, Y., Pérez, G., Jiménez, J. (2016). *Modelo para la evaluación de desempeño de los controles de un SGSI basado en el estándar ISO/IEC 27001*. Colombia. Universidad Nacional de Colombia. VIII Congreso Internacional de Computación y Telecomunicaciones. https://bit.ly/3o5QLNP

BSI Group México. (2013). *Pasando de ISO / IEC 27001: 2005 a ISO / IEC 27001: 2013. El nuevo estándar internacional para los sistemas de gestión de seguridad de la información*. https://bit.ly/39OAIig

Carvajal, D., Cardona, A. y Valencia, F. (2019). Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana. Entre Ciencia e Ingeniería, 13(25), 68-76. https://bit.ly/3sGppRU

Carvalho, C. y Marques, E. (2019). *Adapting ISO 27001 to a Public Institution*. 14th Iberian Conference on Information Systems and Technologies. Portugal. https://bit.ly/3iAiPrE

Chaparro, M. (2016). *Elaboración de un plan de implementación de la ISO/IEC 27001:2013 para la unidad de GST*, para (Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones) Universitat Oberta de Catalunya, España. https://bit.ly/2LRmsNN

Cuatrecasas, L. (2010). *Gestión Integral de la Calidad. Implantación, Control y certificación*. España: Profit editorial.

Eito-Brun, R. y Calleja, C. (2020). *La gestión documental en los modelos de gobernanza TIC: presencia y visibilidad de la normativa internacional en el modelo de referencia COBIT*. Revista Española de Documentación Científica, 43(3), e272. https://bit.ly/3o3vkwS

Enjoy Safer Tecnology – ESET. (2019). *Reporte de Latinoamérica 2019. Las amenazas informáticas que más afectaron a los países de América Latina*. https://bit.ly/2LTRG71

Foro Económico Mundial – FEM. (2020). *The Global Risks Report 2020*. https://bit.ly/2Y5KcQB

Franch, K. y Guerra Bretaña, C. (2016). Las normas ISO 9000: una mirada desde la gestión del conocimiento, la información, innovación y el aprendizaje organizacional. Cofin Habana, 10(2), 29-54. https://bit.ly/2XWvTxS

García, M., Quispe, C. y Ráez, L. (2003). Mejora Continua de la Calidad en los Procesos. Industrial Data, 6(1), 089-094. https://bit.ly/3cbjBKz

Gómez, C. (2020). *Diseñar un Sistema de Gestión de la Seguridad de la Información para la Empresa Qwerty S.A a partir de la Norma ISO 27001*, para (Proyecto para especialidad). Universidad Nacional Abierta y Distancia, Colombia. https://bit.ly/39ShNmQ

Gómez, S. (2012). *Metodología de la investigación*. 1° edición. México: Editorial Red Tercer Milenio.

Hayes, B. (1999). *Como medir la satisfacción del cliente: desarrollo y utilización de cuestionarios*. 2° edición. España: Gestión 2000.

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la investigación*. 6° edición. México: McGraw-Hill.

Humphreys, E. (2016). *Implementing the ISO/IEC 27001 ISMS Standard*. Second Edition. Artech House. Boston-Londres.

Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - Indecopi (2014). *NTP-ISO/IEC 27001:2014 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos*.

Interpol (2020). *Panorama Mundial de la Ciberamenaza relacionada con la COVID-19.* https://bit.ly/2XVPIFw

Kosutic, D. (2017). *Managing ISO Documentation: A Plain English Guide*. First Edition. Advisera Expert Solutions Ltd Zagreb, Croatia.

Mahecha, M. y Coello, G. (2016). *Desarrollo de un Sistema de Información para Gestionar la implantación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información basado en la norma ISO 27001:2013, para* (Tesis de maestro) Escuela Superior Politécnica del Litoral, Ecuador. https://bit.ly/3iBzZVB

Malwarebytes (2019). *El ransomware en empresas aumentó un 200%, según Malwarebytes*. https://bit.ly/3sTsQVA

Ministerio de Trabajo. (2020). Decreto Supremo Nº 010- 2020-TR (24/03/2020), *decreto supremo que desarrolla disposiciones para el Sector Privado, sobre el trabajo remoto previsto en el Decreto de Urgencia N° 026-2020, Decreto de Urgencia que establece medidas excepcionales y temporales para prevenir la propagación del COVID – 19 y de manera supletoria se aplica para las entidades del sector público. https://bit.ly/39Ufn7d*

Muñoz, L. (2020). *Análisis de las normas ISO 9001:2015, NTC 14001:2015, ISO 45001-2018, NTC-ISO-IEC 27001 frente a la gestión documental del Fondo Rotatorio de la Policía*, para (Tesis de grado profesional). Universidad de La Salle, España. https://bit.ly/3qCNWW1

Najar, J. y Suárez, N. (2015). *La seguridad de la información: un activo valioso de la organización*. Revista Vínculos. https://bit.ly/360jsp2

Najar, J. (2016). Exposición del activo más valioso de la organización, la "información". Revista VISIÓN ELECTRÓNICA. https://bit.ly/3sOVMxE

National Cyber Security Centre – NCSC. (2019). *Las 10 contraseñas más comunes en 2019*. https://bbc.in/2XW7Oay

Noguera, I. (2003). *Tesis de Postgrado Proyecto, elaboración, metodología y sustentación*. 1° Edición: Lima: Editorial EDDILI.

OCDE (2012). *The Role of the 2002 Security Guidelines: Towards Cybersecurity for an Open and Interconnected Economy*, OECD Digital Economy Papers, No. 209, OECD Publishing, Paris. https://bit.ly/3qJp3lj

Organización Internacional para la Normalización – ISO, Comisión Electrotécnica Internacional – IEC. (2013). ISO/IEC 27001:2013/COR 1 Information technology – Security techniques – Information security management systems – Requirements.

Pérez, J. (2012). *Gestión de Procesos*. España: ESIC Editorial.

Presidencia de Consejo de Ministros – PCM. (2014). Resolución Ministerial N° 004-2016-PCM (08/01/2016), *Resolución que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades del sector público. Lima, Perú. https://bit.ly/2Y25SNL*

Presidencia de la República (2020). Decreto de Urgencia N° 006-2020(09/01/2020), *decreto de urgencia que crea el sistema nacional de transformación digital del estado peruano y deroga, el cual sustituye al Sistema Nacional de Informática del Perú. https://bit.ly/3bUParP*

Presidencia de la República (2020). Decreto de Urgencia N° 007-2020(09/01/2020), *Decreto de urgencia que aprueba el marco de confianza digital*. *https://bit.ly/3iyO9a7*

Presidencia de la República (2020). Decreto de Urgencia N° 026-2020(15/03/2020), *decreto de urgencia que establece diversas medidas excepcionales y temporales para prevenir la propagación del coronavirus (COVID-19) en el territorio nacional peruano.* https://bit.ly/3bZ4kMs

PricewaterhouseCoopers – PWC. (2019). *Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018*. https://pwc.to/3nXRAYY

Rivera, C., Felipe, A. y Nuñez, F. (2019). *Esquema de ISO 27001 Sistema de Gestión de la Seguridad de la Información*. Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla, 7(13), 28-29. https://bit.ly/3pdIEQQ

Rodríguez, J. (2017). *Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO27001 para laboratorios servicios farmacéuticos de calidad SFC LTDA*, para (Título de especialista) Universidad Nacional Abierta y a Distancia, Colombia. https://bit.ly/2Y1GAPC

Rodríguez, M. y Umenza, A. (2018). *NORMA ISO 27001:2013: Sistema de gestión de seguridad de la información ISO 27001:2013. Colombia.* Universidad Autónoma de Occidente. https://bit.ly/3bZZ5wi

Sanchez, H. (1998). *Metodología y Diseño en la Investigación Científica*. Perú: Edit. Mantaro.

Shojaie, B., Federrath, H. y Saberi, I. (2014). *Evaluating the Effectiveness of ISO 27001: 2013 Based on Annex A. 9th International Conference on Availability, Reliability and Security*. Alemania. University of Hamburg. https://bit.ly/391f0IE

Valencia, F. y Orozco, M. (2017). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000*. Revista Ibérica de Sistemas y Tecnologías de Información, (22), 73-88. https://bit.ly/35WhUfJ

Vásquez, J. (2018). *Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI*, para (Tesis de título

profesional de Ingeniero Industrial) Universidad Nacional Mayor de San Marcos, Perú. https://bit.ly/2NsJuLt

Vergara, O. (2019). *Mejorando la Implantación de la ISO 27001. Mejorando la Implantación de la ISO 27001 en las Organizaciones*. Bogotá D.C. Universidad Piloto de Colombia Carrera 9 No. 45A – 44. https://bit.ly/3ixKkSs

Viveros, A. (2017). *Planeación y ejecución de la auditoría interna del SGSI de Password Consulting Services bajo la norma NTC-ISO/IEC 27001:2013 y plan de acción de las no conformidades encontradas*, para (Tesis de título profesional de Especialista en Seguridad Informática) Universidad Piloto de Colombia, Colombia. https://bit.ly/362pzJP

ANEXOS

Anexo 1: Matriz de operacionalización de variable

Variables	Definición conceptual	Definición operacional	Dimensiones	Indicadores	Items	Escala de medición	Niveles
V1: NTP-ISO/IEC-27001:2014.	Es el recojo de la percepción sobre la implementación de la NTP ISO/IEC 27001:2014 en base a la información documentada requeridos por la norma y por los que establezcan las entidades de los sectores del poder ejecutivo del nivel de gobierno central (integrado).	Es el recojo de la percepción sobre la implementación de las cláusulas relacionadas a la Planificación (Planear) en la que se establece el SGSI definiendo su alcance, de Ejecución (Hacer) en la que se opera el SGSI, de Verificación (Verificar) en la que se identifican brechas entre lo planificado y lo ejecutado y de mejora continua (actuar) en la que se aplican cambios en la ejecución para volver a planificar y reiniciar el ciclo del SGSI según la NTP ISO/IEC 27001:2014, por medio de la técnica de la encuesta y de un cuestionario de preguntas cerradas. Mahecha y Coello (2016)	Planificación	4.3. Alcance del SGSI	1-7	Ordinal	Mala Regular Buena
				5.2. Política de seguridad	8		
				5.3. Roles, responsabilidades y autoridades organizacionales	9-10		
				6.1.2. Valoración del riesgo de seguridad de la información	11-13		
				6.1.3. Tratamiento de riesgos de seguridad de la información	14-15		
				6.2. Objetivos de seguridad de la información	16		
				7.1. Recursos	17		
				7.2. Competencia	18-20		
				7.3. Concientización	21-22		
				7.4. Comunicación	23-25		
				7.5.1. Información documentada - Generalidades	26		
				7.5.2. Creación y actualización	27		
				7.5.3. Información documentada	28		
			Ejecución	8.1. Planificación y control operacional	29		
				8.2. Evaluación de riesgos de seguridad de la información	30-31		
				8.3. Tratamiento de riesgos de seguridad de la información	32		
				9.1. Monitoreo, medición, análisis y evaluación	33		
			Verificación	9.2. Auditoría interna	34-35		
				9.3. Revisión por la gerencia	36		
			Mejora Continua	10.1. No conformidades y acción correctiva	37-39		
				10.2. Mejora continua	40		

Anexo 2: Instrumento de recolección de datos

Estimado(a) encuestado(a), la presente encuesta permitirá identificar la percepción acerca de la implementación de los Sistemas de Gestión de Seguridad de la Información-SGSI en base a los requisitos de la NTP ISO/IEC 27001:2014 en entidades del Poder Ejecutivo del estado peruano.

Instrucciones:

- Las respuestas seleccionadas serán enviadas al correo electrónico que proporcione.
- En las preguntas que no exista avance en la implementación, puede elegir la opción 4 - MUY POCO.
- Considerando los criterios éticos de la investigación los resultados serán mostrados en conjunto y de manera anónima.
- Las respuestas son a título personal.
- La encuesta mide la percepción y no el grado de cumplimiento de la norma ISO 27001.

Escala:

1	2	3	4	5
Muy Poco	Poco	Regular	Mucho	Muchísimo

Indicador		ítems		1	2	3	4	5
DIMENSIÓN 1: Planificación								
1	4.3. Alcance del SGSI	1	La situación externa contemplada en el SGSI contribuye en la planificación de la seguridad de la información de su entidad.					
		2	El SGSI contribuye al cumplimiento de los planes y normatividad interna de su entidad.					
		3	El SGSI atiende las necesidades de seguridad de la información de los procesos misionales y estratégicos de su entidad.					
		4	El SGSI atiende las necesidades de seguridad de la información en los servicios brindados a la ciudadanía por su entidad.					
		5	El SGSI de su entidad está contribuyendo a generar confianza con otras entidades públicas y privadas.					
		6	El SGSI de su entidad contribuye a una gestión adecuada de las relaciones comerciales y/o de cooperación con entidades externas.					
		7	El alcance del SGSI vela por la seguridad de la información relacionada a los procesos principales de la entidad.					
2	5.2. Política de seguridad	8	La política de seguridad promueve el compromiso para que los integrantes del SGSI contribuyan con la seguridad de la información de su entidad.					

Indicador		ítems		1	2	3	4	5
3	5.3. Roles, responsabilidades y autoridades organizacionales	9	Las responsabilidades definidas en el SGSI están alineadas y/o complementan a las del ROF, POI u otras normas de su entidad.					
		10	Las responsabilidades definidas en el SGSI en su entidad están alineadas y/o complementan a las establecidas en los contratos, convenios, tupas o normatividad externa.					
4	6.1.2. Valoración del riesgo de seguridad de la información	11	La metodología de gestión de riesgos contribuye a la gestión del conocimiento de la seguridad de la información de su entidad.					
		12	Las amenazas, vulnerabilidades y riesgos de seguridad de la información identificados contribuyen a afrontar el contexto actual de su entidad.					
		13	Los riesgos de seguridad de la información analizados y evaluados viabilizan contratos o convenios para adquirir nuevos bienes o servicios en su entidad.					
5	6.1.3. Tratamiento de riesgos de seguridad de la información	14	El plan de tratamiento de riesgos de seguridad de la información contribuye a tener una adecuada asignación y ejecución de recursos.					
		15	Los controles de seguridad aplicados contribuyen a mantener la seguridad de la información de su entidad.					
6	6.2. Objetivos de seguridad de la información	16	Los objetivos de seguridad de la información contribuyen a planificar adecuadamente las tareas en el Plan Operativo Institucional.					
7	7.1. Recursos	17	La planificación de tareas y asignación de recursos en el Plan Operativo Institucional contribuyen a implementar y mejorar la seguridad de la información de su entidad.					
8	7.2. Competencia	18	Los perfiles de puestos requeridos para la implementación del SGSI aseguran una adecuada gestión de la seguridad de la información de su entidad.					
		19	El registro de las competencias de los implementadores del SGSI contribuyen a la gestión del conocimiento de la seguridad de la información de su entidad.					
		20	El Plan de Desarrollo de Personas contribuye a mejorar la seguridad de la información de su entidad.					
9	7.3. Concientización	21	La inducción al personal nuevo sobre el SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.					
		22	La guía para usuarios finales del SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.					
10	7.4. Comunicación	23	El listado de documentos del SGSI contribuye a la difusión adecuada de los documentos a nivel interno y externo de su entidad.					
		24	La intranet, el sistema documental y correos masivos al personal contribuyen a las comunicaciones internas que gestionan la seguridad de la información de su entidad.					
		25	El portal .Gob.pe, el portal de transparencia, los documentos y correos a externos contribuyen a las comunicaciones externas que gestionan la seguridad de la información de su entidad.					

Indicador		ítems		1	2	3	4	5
11	7.5.1. Información documentada - Generalidades	26	El listado de documentos requeridos por la NTP-ISO/IEC-27001:2014 y otros documentos contribuyen a gestionar adecuadamente la seguridad de la información de su entidad.					
12	7.5.2. Creación y actualización	27	El procedimiento de Gestión de Documentos del SGSI contribuye a gestionar adecuadamente la seguridad de la información de su entidad.					
13	7.5.3. Información documentada	28	El listado de los documentos externos contribuye a mantener la seguridad de la información de su entidad.					
DIMENSIÓN 2: Ejecución								
14	8.1. Planificación y control operacional	29	La formulación y seguimiento de las tareas del Plan Operativo Institucional ayudan a mejorar la seguridad de la información de su entidad.					
15	8.2. Evaluación de riesgos de seguridad de la información	30	La identificación de nuevas amenazas, vulnerabilidades y riesgos de seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad.					
		31	El análisis y evaluación de nuevos riesgos de seguridad de la información producto del monitoreo del SGSI respaldan la suscripción de nuevos contratos, convenios o adendas.					
16	8.3. Tratamiento de riesgos de seguridad de la información	32	El resultado del tratamiento de riegos de seguridad de la información ayuda a medir la efectividad de los contratos, convenios y planes ejecutados en su entidad.					
DIMENSIÓN 3: Verificación								
17	9.1. Monitoreo, medición, análisis y evaluación	33	Los indicadores, metas y la medición del cumplimiento de los objetivos de la política, procesos y controles de seguridad contribuyen a mejorar la seguridad de la información de su entidad.					
18	9.2. Auditoría Interna	34	El procedimiento y/o programa de Auditorías Internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.					
		35	La documentación de los hallazgos de las auditorías internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.					
19	9.3. Revisión por la gerencia	36	Los informes que miden el progreso del SGSI suscritos por el Comité de Gobierno Digital contribuyen a mejorar la seguridad de la información de su entidad.					
DIMENSIÓN 4: Mejora Continua								
20	10.1. No conformidades y acción correctiva	37	Las no conformidades de los requisitos de la norma ayudan a mejorar la seguridad de la información de su entidad.					
		38	Los planes de acción ayudan a mejorar la seguridad de la información de su entidad.					
		39	Las acciones correctivas implementadas al SGSI ayudan a mejorar la seguridad de la información de su entidad.					
21	10.2. Mejora continua	40	Informar de manera frecuente las acciones de mejora continua del SGSI ayuda a la seguridad de la información de su entidad.					

Anexo 3: Validación del instrumento por el experto

Validación de Experto 1: Dr. Alejandro Ramírez Ríos

MATRIZ DE OPERACIONALIZACIÓN DE LAS VARIABLES

VARIABLES	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA DE MEDICION
V1: Percepción de la NTP-ISO/IEC-27001:2014 en base a la información documentada	Es la percepción de la implementación del Sistemas de Gestión de Seguridad de la Información según la NTP ISO/IEC 27001:2014 tomando como referencia la información documentada requerida por el estándar ISO 27001 y los determinados por las entidades del gobierno central (integrado).	Es la medición de la percepción de la implementación de las cláusulas de Planificación Ejecución, Verificación y mejora continua según la NTP ISO/IEC 27001:2014, por medio de la técnica de la encuesta y de un cuestionario de preguntas cerradas en base a la información documentada establecida en la norma citada.	Planificación	4.3. Alcance del SGSI 5.2. Política de seguridad 5.3. Roles, responsabilidades y autoridades organizacionales 6.1.2. Valoración del riesgo de seguridad de la información 6.1.3. Tratamiento de riesgos de seguridad de la información 6.2. Objetivos de seguridad de la información 7.1. Recursos 7.2. Competencia 7.3. Concientización 7.4. Comunicación 7.5.1. Información documentada - Generalidades 7.5.2. Creación y actualización 7.5.3. Información documentada	Ordinal, con respuestas del tipo Likert 1 – Muy Poco 2 – Poco 3 – Regular 4 – Mucho 5 – Muchísimo ELIMINAR
			Ejecución	8.1. Planificación y control operacional 8.2. Evaluación de riesgos de seguridad de la información 8.3. Tratamiento de riesgos de seguridad de la información	
			Verificación	9.1. Monitoreo, medición, análisis y evaluación 9.2. Auditoría interna 9.3. Revisión por la gerencia	
			Mejora Continua	10.1. No conformidades y acción correctiva 10.2. Mejora continua	

Nº	Dirección del ítem	DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
DIMENSIÓN 1: Planificación			Si	No	Si	No	Si	No	
1	4.2. Alcance del SGSI	La situación externa contemplada en el SGSI contribuye en la planificación de la seguridad de la información de su entidad.	X		X		X		
2		El SGSI contribuye al cumplimiento de los planes y normatividad interna de su entidad.	X		X		X		
3		El SGSI atiende las necesidades de seguridad de la información de los procesos misionales y estratégicos de su entidad.	X		X		X		
4		El SGSI atiende las necesidades de seguridad de la información en los servicios brindados a la ciudadanía por su entidad.	X		X		X		
5		El SGSI de su entidad está contribuyendo a generar confianza con otras entidades públicas y privadas.	X		X		X		
6		El SGSI de su entidad contribuye a una gestión adecuada de las relaciones comerciales y/o de cooperación con entidades externas.	X		X		X		
7		El alcance del SGSI vela por la seguridad de la información relacionada a los procesos principales de la entidad.	X		X		X		
8	5.2. Política de seguridad	La política de seguridad facilita que los integrantes del SGSI contribuyan con la seguridad de la información de su entidad.	X		X		X		
9	5.3. Roles, responsabilidades y autoridades organizacionales	Las responsabilidades definidas en el SGSI están alineadas y/o complementan a las establecidas en el ROF u otras normas de su entidad.	X		X		X		
10		Las responsabilidades definidas en el SGSI en su entidad están alineadas y/o complementan a las establecidas en los contratos, convenios, tupas o normatividad externa.	X		X		X		
11	6.1.2. Valoración del riesgo de seguridad de la información	La metodología de gestión de riesgos contribuye a la gestión del conocimiento de la seguridad de la información de su entidad.	X		X		X		
12		Las amenazas, vulnerabilidades y riesgos de seguridad de la información identificadas contribuyen a afrontar el contexto actual de su entidad.	X		X		X		
13		Los riesgos de seguridad de la información analizados y evaluados viabilizan contratos o convenios para adquirir nuevos bienes o servicios en su entidad.	X		X		X		
14	6.1.3. Tratamiento de riesgos de seguridad de la información	El plan de tratamiento de riesgos de seguridad de la información contribuye a tener una adecuada asignación y ejecución de recursos.	X		X		X		
15		Los controles de seguridad aplicados contribuyen a mantener la seguridad de la información de su entidad.	X		X		X		
16	6.2. Objetivos de seguridad de la información	Los objetivos de seguridad de la información contribuyen a planificar adecuadamente las tareas en el Plan Operativo Institucional.	X		X		X		
17	7.1. Recursos	La planificación de tareas y asignación de recursos en el Plan Operativo Institucional contribuyen a implementar y mejorar la seguridad de la información de su entidad.	X		X		X		

Nº	Dirección del ítem	DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
18	7.2. Competencia	Los perfiles de puestos requeridos para la implementación del SGSI aseguran una adecuada gestión de la seguridad de la información de su entidad.	X		X		X		
19		El registro de las competencias de los implementadores del SGSI contribuyen a la gestión del conocimiento de la seguridad de la información de su entidad.	X		X		X		
20		El Plan de Desarrollo de Personas contribuye a la mejorar la seguridad de la información de su entidad.	X		X		X		
21	7.3. Concientización	La inducción al personal nuevo sobre el SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.	X		X		X		
22		La guía para usuarios finales del SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.	X		X		X		
23	7.4. Comunicación	El listado de documentos del SGSI contribuye a la difusión adecuada de los documentos a nivel interno y externo de su entidad.	X		X		X		
24	7.5.1. Información documentada - Generalidades	El listado de documentos requeridos por la NTP-ISO/IEC-27001:2014 y otros documentos contribuyen a gestionar adecuadamente la seguridad de la información de su entidad.	X		X		X		
25	7.5.2. Creación y actualización	El procedimiento de Gestión de Documentos del SGSI documentos a gestionar adecuadamente la seguridad de la información de su entidad.	X		X		X		
23	7.5.3. Información documentada	El listado de los documentos externos contribuye a mantener la seguridad de la información de su entidad.	X		X		X		
DIMENSIÓN 2: Ejecución			Si	No	Si	No	Si	No	
24	8.1. Planificación y control operacional	La formulación y seguimiento de las tareas del Plan Operativo Institucional ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
25	8.2. Evaluación de riesgos de seguridad de la información	La identificación de nuevas amenazas, vulnerabilidades y riesgos de seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad.	X		X		X		
26		El análisis y evaluación de nuevos riesgos de seguridad de la información producto del monitoreo del SGSI respaldan la suscripción de nuevos contratos, convenios o adendas.	X		X		X		
27	8.3. Tratamiento de riesgos de seguridad de la información	El resultado del tratamiento de riegos de seguridad de la información ayuda a medir la efectividad de los contratos, convenios y planes ejecutados en su entidad.	X		X		X		
DIMENSIÓN 3: Verificación			Si	No	Si	No	Si	No	
29	9.1. Monitoreo, medición, análisis y evaluación	Los indicadores, metas y la medición del cumplimiento de los objetivos de la política, procesos y controles contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
30	9.2. Auditoría Interna	El procedimiento y/o programa de Auditorías Internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.	X		X		X		
31		La documentación de los hallazgos de las auditorías internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.	X		X		X		
32	9.3. Revisión por la gerencia	Los informes que miden el progreso del SGSI suscritos por el Comité de Gobierno Digital contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
DIMENSIÓN 4: Mejora Continua			Si	No	Si	No	Si	No	
33	10.1. No conformidades y acción correctiva	Las no conformidades de los requisitos de la norma ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
34		Los planes de acción ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
35		Las acciones correctivas implementadas al SGSI ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
36	10.2. Mejora continua	Informar de manera frecuente las acciones de mejora continua del SGSI ayuda a la seguridad de la información de su entidad.	X		X		X		

Observaciones:

_____

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

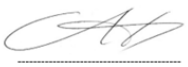
Apellidos y nombres del juez validador: Dr. Alejandro Ramírez Ríos

DNI: 07191553

Especialidad del validador: Dr. en Ciencias de la Educación

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

...22..... de diciembre del 2020



Firma del Experto Informante

Validación de Experto 2: Mg. Elvis Gonzalo Malpartida Asencio

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA PERCEPCIÓN DE LA NTP-ISO/IEC-27001:2014 EN BASE A LA INFORMACIÓN DOCUMENTADA

Nº	Dirección del ítem	DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
DIMENSIÓN 1: Planificación			Si	No	Si	No	Si	No	
1	4.3.~~4.2~~ Alcance del SGSI	La situación externa contemplada en el SGSI contribuye en la planificación de la seguridad de la información de su entidad.	X		X		X		
2		El SGSI contribuye al cumplimiento de los planes y normatividad interna de su entidad.	X		X		X		
3		El SGSI atiende las necesidades de seguridad de la información de los procesos misionales y estratégicos de su entidad.	X		X		X		
4		El SGSI atiende las necesidades de seguridad de la información en los servicios brindados a la ciudadanía por su entidad.	X		X		X		
5		El SGSI de su entidad está contribuyendo a generar confianza con otras entidades públicas y privadas.	X		X		X		
6		El SGSI de su entidad contribuye a una gestión adecuada de las relaciones comerciales y/o de cooperación con entidades externas.	X		X		X		
7		El alcance del SGSI vela por la seguridad de la información relacionada a los procesos principales de la entidad.	X		X		X		
8	5.2. Política de seguridad	La política de seguridad promueve el compromiso para ~~facilita~~ que los integrantes del SGSI contribuyan con la seguridad de la información de su entidad.	X		X		X		
9	5.3. Roles, responsabilidades y autoridades organizacionales	Las responsabilidades definidas en el SGSI están alineadas y/o complementan a las del ROF, POI u otras normas de su entidad.	X		X		X		
10		Las responsabilidades definidas en el SGSI en su entidad están alineadas y/o complementan a las establecidas en los contratos, convenios, tupas o normatividad externa.	X		X		X		
11	6.1.2. Valoración del riesgo de seguridad de la información	La metodología de gestión de riesgos contribuye a la gestión del conocimiento de la seguridad de la información de su entidad.	X		X		X		
12		Las amenazas, vulnerabilidades y riesgos de seguridad de la información identificados contribuyen a afrontar el contexto actual de su entidad.	X		X		X		
13		Los riesgos de seguridad de la información analizados y evaluados viabilizan contratos o convenios para adquirir nuevos bienes o servicios en su entidad.	X		X		X		
14	6.1.3. Tratamiento de riesgos de seguridad de la información	El plan de tratamiento de riesgos de seguridad de la información contribuye a tener una adecuada asignación y ejecución de recursos.	X		X		X		
15		Los controles de seguridad aplicados contribuyen a mantener la seguridad de la información de su entidad.	X		X		X		
16	6.2. Objetivos de seguridad de la información	Los objetivos de seguridad de la información contribuyen a planificar adecuadamente las tareas en el Plan Operativo Institucional.	X		X		X		
17	7.1. Recursos	La planificación de tareas y asignación de recursos en el Plan Operativo Institucional contribuyen a implementar y mejorar la seguridad de la información de su entidad.	X		X		X		
18	7.2. Competencia	Los perfiles de puestos requeridos para la implementación del SGSI aseguran una adecuada gestión de la seguridad de la información de su entidad.	X		X		X		
19		El registro de las competencias de los implementadores del SGSI contribuyen a la gestión del conocimiento de la seguridad de la información de su entidad.	X		X		X		
20		El Plan de Desarrollo de Personas contribuye a la mejorar la seguridad de la información de su entidad.	X		X		X		
21	7.3. Concientización	La inducción al personal nuevo sobre el SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.	X		X		X		
22		La guía para usuarios finales del SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.	X		X		X		
23	7.4. Comunicación	El listado de documentos del SGSI contribuye a la difusión adecuada de los documentos a nivel interno y externo de su entidad. Transparencia, Gob.pe, intranet, mailing, Sistema documental	X		X		X		
24	7.5.1. Información documentada - Generalidades	El listado de documentos requeridos por la NTP-ISO/IEC-27001:2014 y otros documentos contribuyen a gestionar adecuadamente la seguridad de la información de su entidad.	X		X		X		
25	7.5.2. Creación y actualización	El procedimiento de Gestión de Documentos del SGSI contribuye ~~documentos~~ a gestionar adecuadamente la seguridad de la información de su entidad.	X		X		X		
26	7.5.3. Información documentada	El listado de los documentos externos contribuye a mantener la seguridad de la información de su entidad.	X		X		X		
DIMENSIÓN 2: Ejecución			Si	No	Si	No	Si	No	
27	8.1. Planificación y control operacional	La formulación y seguimiento de las tareas del Plan Operativo Institucional ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
28	8.2. Evaluación de riesgos de seguridad de la información	La identificación de nuevas amenazas, vulnerabilidades y riesgos de seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad.	X		X		X		
29		El análisis y evaluación de nuevos riesgos de seguridad de la información producto del monitoreo del SGSI respaldan la suscripción de nuevos contratos, convenios o adendas.	X		X		X		
30	8.3. Tratamiento de riesgos de seguridad de la información	El resultado del tratamiento de riesgos de seguridad de la información ayuda a medir la efectividad de los contratos, convenios y planes ejecutados en su entidad.	X		X		X		
DIMENSION 3: Verificación			Si	No	Si	No	Si	No	
31	9.1. Monitoreo, medición, análisis y evaluación	Los indicadores, metas y la medición del cumplimiento de los objetivos de la política, procesos y controles de seguridad contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
32	9.2. Auditoría Interna	El procedimiento y/o programa de Auditorías Internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.	X		X		X		
33		La documentación de los hallazgos de las auditorías internas del SGSI contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
34	9.3. Revisión por la gerencia	Los informes que miden el progreso del SGSI suscritos por el Comité de Gobierno Digital contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
DIMENSIÓN 4: Mejora Continua			Si	No	Si	No	Si	No	
35	10.1. No conformidades y acción correctiva	Las no conformidades de los requisitos de la norma ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
36		Los planes de acción ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
37		Las acciones correctivas implementadas al SGSI ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
38	10.2. Mejora continua	Informar de manera frecuente las acciones de mejora continua del SGSI ayuda a la seguridad de la información de su entidad.	X		X		X		

Observaciones:

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

Apellidos y nombres del juez validador Mg. Elvis Gonzalo Malpartida Asencio

DNI: 10044323

Especialidad del validador: Ingeniero Electrónico con maestría en Gestión Pública

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

30 de diciembre del 2020

Firma del Experto Informante

Validación de Experto 3: Dr. Nicolas Álvarez Carrillo

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA PERCEPCIÓN DE LA NTP-ISO/IEC-27001:2014 EN BASE A LA INFORMACIÓN DOCUMENTADA|

Nº	Dirección del ítem	DIMENSIONES / ítems	Pertinencia [1]		Relevancia [2]		Claridad [3]		Sugerencias
DIMENSIÓN 1: Planificación			Si	No	Si	No	Si	No	
1	4.2. Alcance del SGSI	La situación externa contemplada en el SGSI contribuye en la planificación de la seguridad de la información de su entidad.	X		X		X		
2		El SGSI contribuye al cumplimiento de los planes y normatividad interna de su entidad.	X		X		X		
3		El SGSI atiende las necesidades de seguridad de la información de los procesos misionales y estratégicos de su entidad.	X		X		X		
4		El SGSI atiende las necesidades de seguridad de la información en los servicios brindados a la ciudadanía por su entidad.	X		X		X		
5		El SGSI de su entidad está contribuyendo a generar confianza con otras entidades públicas y privadas.	X		X		X		
6		El SGSI de su entidad contribuye a una gestión adecuada de las relaciones comerciales y/o de cooperación con entidades externas.	X		X		X		
7		El alcance del SGSI vela por la seguridad de la información relacionada a los procesos principales de la entidad.	X		X		X		
8	5.2. Política de seguridad	La política de seguridad facilita que los integrantes del SGSI contribuyan con la seguridad de la información de su entidad.	X		X		X		
9	5.3. Roles, responsabilidades y autoridades organizacionales	Las responsabilidades definidas en el SGSI están alineadas y/o complementan a las establecidas en el ROF u otras normas de su entidad.	X		X		X		
10		Las responsabilidades definidas en el SGSI en su entidad están alineadas y/o complementan a las establecidas en los contratos, convenios, tupas o normatividad externa.	X		X		X		
11	6.1.2. Valoración del riesgo de seguridad de la información	La metodología de gestión de riesgos contribuye a la gestión del conocimiento de la seguridad de la información de su entidad.	X		X		X		
12		Las amenazas, vulnerabilidades y riesgos de seguridad de la información identificadas contribuyen a afrontar el contexto actual de su entidad.	X		X		X		
13		Los riesgos de seguridad de la información analizados y evaluados viabilizan contratos o convenios para adquirir nuevos bienes o servicios en su entidad.	X		X		X		
14	6.1.3. Tratamiento de riesgos de seguridad de la información	El plan de tratamiento de riesgos de seguridad de la información contribuye a tener una adecuada asignación y ejecución de recursos.	X		X		X		
15		Los controles de seguridad aplicados contribuyen a mantener la seguridad de la información de su entidad.	X		X		X		
16	6.2. Objetivos de seguridad de la información	Los objetivos de seguridad de la información contribuyen a planificar adecuadamente las tareas en el Plan Operativo Institucional.	X		X		X		
17	7.1. Recursos	La planificación de tareas y asignación de recursos en el Plan Operativo Institucional contribuyen a implementar y mejorar la seguridad de la información de su entidad.	X		X		X		
18	7.2. Competencia	Los perfiles de puestos requeridos para la implementación del SGSI aseguran una adecuada gestión de la seguridad de la información de su entidad.	X		X		X		
19		El registro de las competencias de los implementadores del SGSI contribuyen a la gestión del conocimiento de la seguridad de la información de su entidad.	X		X		X		
20		El Plan de Desarrollo de Personas contribuye a la mejorar la seguridad de la información de su entidad.	X		X		X		
21	7.3. Concientización	La inducción al personal nuevo sobre el SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.	X		X		X		
22		La guía para usuarios finales del SGSI contribuye a mantener y mejorar la seguridad de la información de su entidad.	X		X		X		
23	7.4. Comunicación	El listado de documentos del SGSI contribuye a la difusión adecuada de los documentos a nivel interno y externo de su entidad.	X		X		X		
24	7.5.1. Información documentada - Generalidades	El listado de documentos requeridos por la NTP-ISO/IEC-27001:2014 y otros documentos contribuyen a gestionar adecuadamente la seguridad de la información de su entidad.	X		X		X		
25	7.5.2. Creación y actualización	El procedimiento de Gestión de Documentos del SGSI documentos a gestionar adecuadamente la seguridad de la información de su entidad.	X		X		X		
23	7.5.3. Información documentada	El listado de los documentos externos contribuye a mantener la seguridad de la información de su entidad.	X		X		X		
DIMENSIÓN 2: Ejecución			Si	No	Si	No	Si	No	
24	8.1. Planificación y control operacional	La formulación y seguimiento de las tareas del Plan Operativo Institucional ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
25	8.2. Evaluación de riesgos de seguridad de la información	La identificación de nuevas amenazas, vulnerabilidades y riesgos de seguridad de la información producto del monitoreo del SGSI contribuyen a afrontar los nuevos contextos de su entidad.	X		X		X		
26		El análisis y evaluación de nuevos riesgos de seguridad de la información producto del monitoreo del SGSI respaldan la suscripción de nuevos contratos, convenios o adendas.	X		X		X		
27	8.3. Tratamiento de riesgos de seguridad de la información	El resultado del tratamiento de riegos de seguridad de la información ayuda a medir la efectividad de los contratos, convenios y planes ejecutados en su entidad.	X		X		X		
DIMENSIÓN 3: Verificación			Si	No	Si	No	Si	No	
29	9.1. Monitoreo, medición, análisis y evaluación	Los indicadores, metas y la medición del cumplimiento de los objetivos de la política, procesos y controles contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
30	9.2. Auditoría Interna	El procedimiento y/o programa de Auditorías Internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.	X		X		X		
31		La documentación de los hallazgos de las auditorías internas del SGSI contribuye a mejorar la seguridad de la información de su entidad.	X		X		X		
		mejorar la seguridad de la información de su entidad.							
32	9.3. Revisión por la gerencia	Los informes que miden el progreso del SGSI suscritos por el Comité de Gobierno Digital contribuyen a mejorar la seguridad de la información de su entidad.	X		X		X		
DIMENSIÓN 4: Mejora Continua			Si	No	Si	No	Si	No	
33	10.1. No conformidades y acción correctiva	Las no conformidades de los requisitos de la norma ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
34		Los planes de acción ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
35		Las acciones correctivas implementadas al SGSI ayudan a mejorar la seguridad de la información de su entidad.	X		X		X		
36	10.2. Mejora continua	Informar de manera frecuente las acciones de mejora continua del SGSI ayuda a la seguridad de la información de su entidad.	X		X		X		

Observaciones:

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

Apellidos y nombres del juez validador: Dr. Nicolas Álvarez Carrillo

DNI: 32736800

Especialidad del validador: DOCENTE MATEMÀTICA, FÌSICA Y COMPUTACIÓN.

[1]**Pertinencia**: El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

22 de diciembre del 2020

Firma del Experto Informante

Anexo 4: Autorización de aplicación del instrumento

Autorización de la Presidencia del Consejo de Ministros – SEGDI - PECERT

PECERT Secretaría de Gobierno Digital 18 ene. 2021 13:03 (hace 4 días) Responder a todos
para mí, Inocencio, Edwing

Estimada Srta. Vanessa Liliana Diaz Lara,

En atención a su solicitud se ha cursado 872 correos.

Inocencio Arsenio Paredes Castillo
PECERT | EQUIPO DE RESPUESTAS ANTE INCIDENTES DE SEGURIDAD DIGITAL NACIONAL
SECRETARIA DE GOBIERNO DIGITAL
PRESIDENCIA DEL CONSEJO DE MINISTROS
(511) 219-7000 Anexo 5109 | +51 9[redacted]
www.gob.pe/7739 | pecert@pcm.gob.pe | iparedes@pcm.gob.pe
Este correo es totalmente confidencial de uso exclusivo de la persona o entidad de destino

De: Liliana <vanessaliliana@gmail.com>
Enviado el: lunes, 4 de enero de 2021 16:22
Para: PCM | PECERT Secretaría de Gobierno Digital. <pecert@pcm.gob.pe>
CC: Inocencio Arsenio Paredes Castillo <iparedes@pcm.gob.pe>
Asunto: Encuesta para investigación sobre la PERCEPCIÓN DE LA IMPLEMENTACIÓN DE LA NTP-ISO/IEC 27001:2014

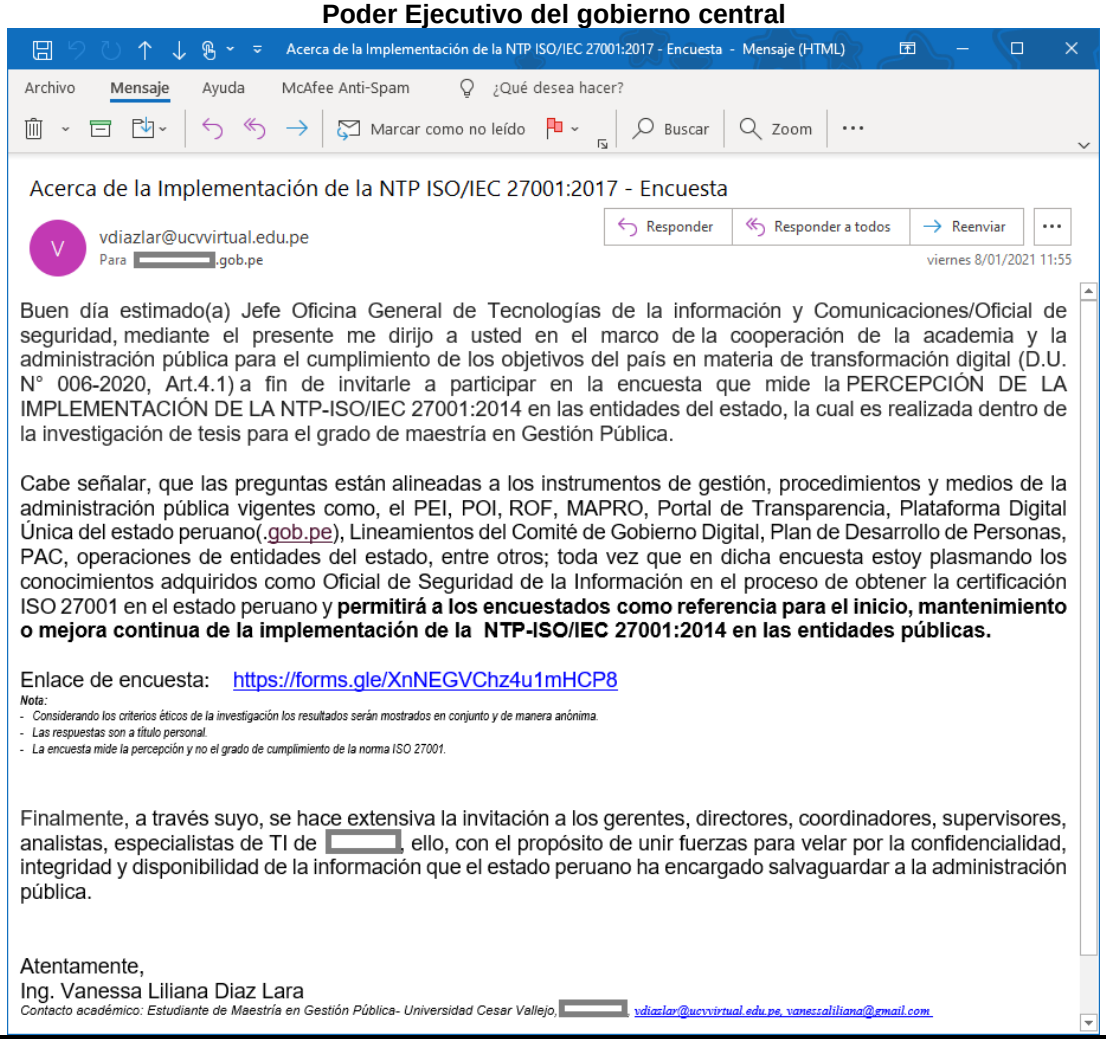
Buenas tardes estimados señores del PECERT, mediante el presente reciban un cordial saludo, me presento en mi calidad de estudiante de maestría en Gestión Pública (adjunto resolución de mi casa de estudios) ; en ese sentido, en el marco de unir fuerzas entre la administración pública y la academia recurro a ustedes a fin de que en su calidad de ente rector en materia digital soliciten a los Oficiales de Seguridad de la Información-CISO que tienen en vuestra base de datos el llenado de la encuesta que permitirá medir la PERCEPCIÓN DE LA IMPLEMENTACIÓN DE LA NTP-ISO/IEC 27001:2014, la cual es dirigida a gerentes, directores, coordinadores, supervisores, analistas, especialistas de TI y cisos del estado peruano. Considerando el respectivo alineamiento a los instrumentos, procedimientos y medios de la administración pública vigente como, el PEI, POI, ROF, MAPRO, Portal de Transparencia, Plataforma Digital Única del estado peruano(.gob.pe), Plan de Desarrollo de Personas, PAC, entre otros.

En ese sentido, agradezco de antemano vuestro valioso apoyo dado que la presente investigación contribuirá a identificar la situación y/o como línea base para que se inicie, continúe o mejore la implementación de los Sistemas de Gestión de la Información a fin de velar por la confidencialidad, integridad y disponibilidad que el estado peruano le ha encargado salvaguardar a la administración pública y se estarán cumpliendo los objetivos del país en materia de transformación digital.(D.U. N° 006-2020, Art.4.1)

https://forms.gle/XnNEGVChz4u1mHCP8

Atentamente,
Ing. Vanessa Liliana Diaz Lara
Datos académicos: Estudiante de Maestría en Gestión Pública- Universidad Cesar Vallejo, Celular[redacted] vanessaliliana@gmail.com

Gestión ante 105 jefes y oficiales de seguridad de la información de las entidades del Poder Ejecutivo del gobierno central



Acerca de la Implementación de la NTP ISO/IEC 27001:2017 - Encuesta - Mensaje (HTML)

Archivo Mensaje Ayuda McAfee Anti-Spam ¿Qué desea hacer?

Marcar como no leído Buscar Zoom

Acerca de la Implementación de la NTP ISO/IEC 27001:2017 - Encuesta

Responder Responder a todos Reenviar

vdiazlar@ucvvirtual.edu.pe
Para [redacted].gob.pe
viernes 8/01/2021 11:55

Buen día estimado(a) Jefe Oficina General de Tecnologías de la información y Comunicaciones/Oficial de seguridad, mediante el presente me dirijo a usted en el marco de la cooperación de la academia y la administración pública para el cumplimiento de los objetivos del país en materia de transformación digital (D.U. N° 006-2020, Art.4.1) a fin de invitarle a participar en la encuesta que mide la PERCEPCIÓN DE LA IMPLEMENTACIÓN DE LA NTP-ISO/IEC 27001:2014 en las entidades del estado, la cual es realizada dentro de la investigación de tesis para el grado de maestría en Gestión Pública.

Cabe señalar, que las preguntas están alineadas a los instrumentos de gestión, procedimientos y medios de la administración pública vigentes como, el PEI, POI, ROF, MAPRO, Portal de Transparencia, Plataforma Digital Única del estado peruano(.gob.pe), Lineamientos del Comité de Gobierno Digital, Plan de Desarrollo de Personas, PAC, operaciones de entidades del estado, entre otros; toda vez que en dicha encuesta estoy plasmando los conocimientos adquiridos como Oficial de Seguridad de la Información en el proceso de obtener la certificación ISO 27001 en el estado peruano y **permitirá a los encuestados como referencia para el inicio, mantenimiento o mejora continua de la implementación de la NTP-ISO/IEC 27001:2014 en las entidades públicas.**

Enlace de encuesta: https://forms.gle/XnNEGVChz4u1mHCP8

Nota:
- *Considerando los criterios éticos de la investigación los resultados serán mostrados en conjunto y de manera anónima.*
- *Las respuestas son a título personal.*
- *La encuesta mide la percepción y no el grado de cumplimiento de la norma ISO 27001.*

Finalmente, a través suyo, se hace extensiva la invitación a los gerentes, directores, coordinadores, supervisores, analistas, especialistas de TI de [redacted], ello, con el propósito de unir fuerzas para velar por la confidencialidad, integridad y disponibilidad de la información que el estado peruano ha encargado salvaguardar a la administración pública.

Atentamente,
Ing. Vanessa Liliana Diaz Lara
Contacto académico: Estudiante de Maestría en Gestión Pública- Universidad Cesar Vallejo, [redacted] vdiazlar@ucvvirtual.edu.pe, vanessaliliana@gmail.com

Anexo 5: Confiabilidad del instrumento

Base de dato de la prueba piloto de la Variable 1: NTP ISO/IEC 27001

	NTP-ISO/IEC 27001:2014																																	
	Planificación																										Ejecución				Verificación				Mejora continua			
	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	33	34	35	36	37	38	39	40
1	4	3	4	4	4	3	3	4	2	3	2	4	4	3	4	3	4	3	3	2	3	3	4	4	4	3	3	3	4	4	4	4	3	5	5	4	3	4	4	4
2	4	4	5	4	5	3	4	5	4	4	5	5	4	4	4	4	4	5	4	5	5	5	5	5	5	5	5	4	5	4	4	4	5	5	5	5	4	5	5	5
3	3	4	3	4	4	3	4	3	4	3	4	4	3	3	4	3	3	4	4	4	4	4	4	4	4	4	4	3	3	4	3	3	4	5	5	4	5	4	4	4
4	4	1	1	1	1	1	1	1	1	1	1	1	1	1	4	1	3	1	1	3	1	3	1	5	5	3	3	1	4	1	1	3	1	5	5	1	1	1	5	5
5	4	5	5	5	5	5	5	5	5	5	5	5	5	4	4	3	4	5	5	5	4	4	5	5	4	5	5	4	3	5	5	5	5	5	5	4	4	4	4	5
6	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	3	3	3	4	4	4	4	4	4	4	4	4	4	3	4	3	3	4	4	4	4	4	4	4	4
8	4	4	4	4	4	3	5	4	3	3	4	4	5	4	5	3	3	4	4	3	5	4	4	4	3	4	3	4	4	5	3	4	5	5	4	4	5	5	5	4
9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
10	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4
11	4	5	5	4	1	1	4	5	3	2	4	4	3	4	4	4	3	2	2	2	4	4	2	4	4	4	4	3	4	4	4	5	5	5	5	5	2	4	5	5
12	4	2	4	4	4	2	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	4
13	4	3	4	4	4	2	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	4	4	4	4	4	5	5	5	4
14	4	4	4	4	4	4	4	4	4	3	3	4	4	4	4	4	4	3	3	3	4	4	3	4	4	4	4	3	4	4	3	4	4	4	4	4	4	5	5	4
15	4	4	5	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	5	5	4	5	5	5
16	4	4	4	4	4	3	4	4	4	2	4	4	3	3	4	3	4	3	3	2	4	2	2	4	4	4	4	3	4	4	3	3	3	5	5	3	5	4	5	4
17	4	4	4	5	5	3	5	4	4	4	3	4	4	4	4	4	3	4	4	4	3	3	3	4	3	4	4	3	4	5	5	4	3	5	4	4	4	4	4	5
18	1	3	4	4	3	3	4	4	3	2	3	4	3	4	4	4	4	4	4	3	4	4	4	4	2	4	4	3	4	4	3	2	4	4	4	4	4	4	4	4
19	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5	4	4	4	4	4	4	4	4	4	4	4	4	4	5
20	3	3	3	3	4	3	4	4	3	3	3	4	3	3	4	3	3	3	3	3	4	4	2	3	3	3	4	3	3	3	3	3	4	3	4	3	4	3	4	3

Estadísticas de total de elemento

	Media de escala si el elemento se ha suprimido	Varianza de escala si el elemento se ha suprimido	Correlación total de elementos corregida	Alfa de Cronbach si el elemento se ha suprimido
VAR00001	134,7000	1799,589	,864	,991
VAR00002	134,8500	1781,818	,849	,991
VAR00003	134,5500	1769,734	,913	,990
VAR00004	134,7500	1770,303	,952	,990
VAR00005	134,9500	1772,366	,843	,991
VAR00006	135,4500	1791,313	,756	,991
VAR00007	134,6000	1771,832	,916	,990
VAR00008	134,7000	1766,221	,934	,990
VAR00009	134,8000	1787,747	,818	,991
VAR00010	135,1000	1787,147	,803	,991
VAR00011	134,9000	1775,358	,884	,990
VAR00012	134,7500	1773,882	,949	,990
VAR00013	135,0000	1792,316	,820	,991
VAR00014	135,2000	1791,958	,836	,991
VAR00015	134,5500	1795,839	,880	,990
VAR00016	135,2000	1799,432	,866	,990
VAR00017	134,9000	1803,463	,873	,991
VAR00018	135,0500	1783,734	,882	,990
VAR00019	135,0500	1782,155	,868	,990
VAR00020	134,9500	1785,103	,777	,991
VAR00021	134,8000	1773,326	,925	,990
VAR00022	135,0500	1790,787	,786	,991
VAR00023	135,0000	1782,737	,854	,990
VAR00024	134,4500	1799,313	,788	,991
VAR00025	134,5500	1801,839	,778	,991
VAR00026	134,6000	1783,726	,965	,990
VAR00027	134,7000	1786,326	,929	,990
VAR00028	135,3000	1803,484	,782	,991
VAR00029	134,8000	1799,432	,791	,991
VAR00030	134,9000	1773,568	,851	,991
VAR00031	135,2500	1795,776	,782	,991
VAR00032	135,0000	1792,000	,823	,991
VAR00033	134,8000	1765,011	,919	,990
VAR00034	134,0500	1792,787	,794	,991
VAR00035	134,1500	1788,450	,800	,991
VAR00036	134,7000	1775,168	,908	,990
VAR00037	134,6500	1778,029	,810	,991
VAR00038	134,4500	1768,261	,913	,990
VAR00039	134,1500	1788,661	,798	,991
VAR00040	134,4000	1795,411	,807	,991

Anexo N° 06: Información Documentada basado en ISO/IEC 27001:2013

Fuente: BSI Group México (2013)

Cláusulas	Información Documentada
1.3	Alcance del SGSI
5.2	Política de seguridad de la información
6.1.2	Proceso de evaluación de riesgos de seguridad de la información
6.1.3	Proceso de tratamiento de riesgos de seguridad de la información
6.1.3 d)	Enunciado de Aplicabilidad
6.2	Objetivos de Seguridad de la Información
7.2 d)	Evidencia de competencia
7.5.1b)	La información documentada determinada por la organización como siendo necesaria para la efectividad del SGSI
8.1	Control y planeación operacional
8.2	Resultados de la evaluación de riesgos de seguridad de la información
8.3	Resultados del tratamiento de riesgos de seguridad de la información
9.1	Evidencia de los resultados del monitoreo y mediciones
9.2 g)	Evidencia de los programas y resultados de auditoria
9.3	Evidencia de los resultados de las revisiones de gestión
10.1 f)	Evidencia de la naturaleza de las no conformidades y cualquier acción tomada subsecuentemente
10.1 g)	Evidencia de los resultados de cualquier acción correctiva

Fuente: Valencia, Orozco (2017)

	Numeral ISO/IEC 27001:2013	Documentación
4.3	Determinación del alcance del SGSI	El alcance debe estar disponible como información documentada
5.2	Política de seguridad	e) La política de seguridad debe estar disponible como información documentada
6.1.2	Valoración de riesgos de seguridad de la información	Información documentada acerca del proceso de valoración de riesgos de la seguridad de la información
6.1.3	Tratamiento de riesgos de seguridad de la información	Información documentada acerca del proceso de tratamiento de los riesgos de seguridad de la información
6.1.3	Declaración de aplicabilidad	d) Declaración de aplicabilidad
6.2	Objetivos de seguridad de la información y planes para lograrlos	Objetivos de la seguridad de la información
7.2	Competencia	Evidencia de la competencia de las personas relacionadas con la seguridad de la información
7.5	Información documentada	b) La que la empresa ha determinado que es necesaria para la eficacia del SGSI
7.5.3	Control de la información documentada	La información documentada de origen externo
8.1	Control y planeación operacional	Información documentada para tener confianza de que los procesos se han llevado a cabo de acuerdo a lo planificado
8.2	Valoración de la seguridad de la información	Resultados de las valoraciones de riesgos de la seguridad de la información
8.3	Tratamiento de riesgos de seguridad de la información	Resultados de los tratamientos de riesgos de la seguridad de la información
9.1	Seguimiento, medición, análisis y evaluación	Evidencia de los resultados del monitoreo y de la medición
9.2	Auditoría interna	g) conservar la información documentada como evidencia de la implementación del programa de auditoría y de los resultados de ésta.
9.3	Revisión por la dirección	Evidencia de los resultados de la revisión por la Dirección
10.1	No conformidades y acciones correctivas	Naturaleza de las no conformidades y cualquier acción posterior tomada
10.1	No conformidades y acciones correctivas	Resultados de cualquier acción correctiva

Anexo 7: Análisis de factores de éxito en la implementación ISO 27001

Factores Críticos de Éxito [2]	Cláusula ISO 27001 [2]	Ciclo PDCA [2]	Entidad Pública A[1]	Entidad Pública B [1]	Promedio [2]
Alineamiento con el Negocio	4.3 Determinar el alcance del sistema de gestión de seguridad de la información 6.2 Objetivos de seguridad de la información y planificación para conseguirlos	Planificación	60%	80%	70%
Soporte de la alta Gerencia	5. Liderazgo	Planificación	40%	70%	55%
Financiamiento (recursos)	7.1 Recursos	Planificación	90%	80%	85%
Estructura organizacional	5.3 Roles, responsabilidades y autoridades organizacionales	Planificación	70%	50%	60%
Personal consiente y entrenado	7.2 Competencia 7.3 Concientización	Planificación	53%	53%	53%
Cultura de seguridad de la información	7.3 Concientización	Planificación	80%	90%	85%
Competencias de TI	7.2 Competencia	Planificación	60%	70%	65%
Administración del riesgo	8.2. Evaluación de riesgos de seguridad de la información 8.3 Tratamiento de riesgos de seguridad de la información	Ejecución	80%	80%	80%
Implementación de Políticas de Seguridad	8.1 Planificación y control operacional	Ejecución	40%	50%	45%
Cumplimiento de Normas	8.1 Planificación y control operacional	Ejecución	90%	70%	80%
Evaluación de la performance	9. Evaluación del Desempeño	Verificación	40%	50%	45%
Evaluación de la Organización	9. Evaluación del Desempeño	Verificación	64%	68%	66%
		Promedio Cláusula de Planificación como factor de éxito			68%
		Promedio Cláusula de Ejecución como factor de éxito			68%
		Promedio Cláusula de Verificación como factor de éxito			56%

Nota: [1]Datos obtenidos de Bayona (2015). [2] Datos analizados en la investiga