Universidad Nacional
Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

IMPLEMENTACIÓN DE UNA METODOLOGÍA PARA AUDITAR LA GESTIÓN INFORMÁTICA EN ENTIDADES PÚBLICAS, SUJETAS AL SISTEMA NACIONAL DE CONTROL

Línea de Investigación:

Sistemas de Información y Optimización

Tesis para optar el grado académico de Maestro en Ingeniera de Sistemas

Autor:
Bonifaz Ocampo, Arturo Enrique

Asesor:
Kaseng Solís, Freddy Lizardo
ORCID: 000-0002-2878-9053

Jurado:
Manrique Suarez, Luis Humberto
Ccasani Allende, Julián
Bazán Briceño, José Luis

Lima – Perú
2022

DEDICATORIA:

A mis padres, que me inculcaron el valor del estudio y la superación.

A mi amigo Isidro QEPD, quien me sumergió en el solitario y poco comprendido pero fascinante mundo de la auditoría.

A los que con su amor hacen felices mis días porque me comprenden y estimulan para llegar a la meta.

AGRADECIMIENTO:

Un agradecimiento muy especial al Dr. Ing. Freddy Lizardo Kaseng Solís QEPD por contribuir con sus conocimientos y experiencia a la materialización de este trabajo de investigación.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El uso deficiente de los recursos públicos, asignados a las oficinas de tecnologías de información de las entidades del estado, por limitaciones burocráticas o desconocimiento del marco normativo que reglamenta los procedimientos; así como la ausencia de un adecuado control interno; trae como consecuencia que la gestión de estas oficinas no sea eficiente ni eficaz; situación que dificulta el logro de los objetivos y metas programadas e incide de manera indirecta en perjuicio de la sociedad. La presente investigación está orientada a diseñar una metodología para optimizar el sistema de control interno de las oficinas de tecnologías de información de las entidades públicas sujetas al Sistema Nacional de Control, bajo el enfoque de mejora continua; para lo cual se utilizaron datos obtenidos como integrante de las Sociedades de Auditoría Externa que realizan acciones de control a sendas entidades del estado peruano y se diseñaron estrategias tendientes a mejorar la organización, racionalizar el uso de la infraestructura de las oficinas de tecnologías de información, mejorar los procesos de adquisición, uso y mantenimiento de los recursos informáticos; así como a aplicar normas de seguridad informática. La recopilación de información se realizó en múltiples entidades públicas auditadas por las Sociedades de Auditoría Externa, de cuya comisión formé parte como Especialista o Experto Informático. Esta data ha servido de evidencia para observar el nulo o reducido avance en la áreas orgánicas encargadas de gestionar tecnologías de información y ha motivado la necesidad de diseñar un sistema que sirva de apoyo a los funcionarios para que su gerenciamiento mejore de manera continua, de tal manera que se puedan desarrollar de forma más rápida, eficiente y oportuna las auditorías de control. Del análisis de los resultados obtenidos podemos concluir que, debido a la implementación de mejores controles; algunas actividades han mejorado en 50% y otras en 100%; de esta manera hemos logrado eficacia en el desempeño de la función pública, menor gasto y por ende presupuesto para desarrollar actividades o proyectos adicionales.

Palabras clave: auditoria informática, control informático, control interno, sistema de control interno.

ABSTRACT

The deficient use of public resources, assigned to the information technology offices of state entities, due to bureaucratic limitations or ignorance of the regulatory framework that regulates the procedures; as well as the absence of adequate internal control; As a consequence, the management of these offices is neither efficient nor effective; situation that makes it difficult to achieve the objectives and goals set and has an indirect impact on society. This research is aimed at designing a methodology to optimize the internal control system of the information technology offices of public entities subject to the National Control System, under the continuous improvement approach; for which data obtained as a member of the External Audit Societies that carry out control actions to various entities of the Peruvian state were used and strategies were designed to improve the organization, rationalize the use of the infrastructure of the information technology offices, improve the processes of acquisition, use and maintenance of computer resources; as well as to apply computer security standards. The collection of information was carried out in multiple public entities audited by the External Audit Societies, of whose commission I was part as a Computer Specialist or Expert. This data has served as evidence to observe the null or reduced progress in the organic areas in charge of managing information technologies and has motivated the need to design a system that supports officials so that their management improves continuously, in such a way that so that control audits can be carried out more quickly, efficiently and in a timely manner. From the analysis of the results obtained we can conclude that, due to the implementation of better controls; some activities have improved by 50% and others by 100%; In this way we have achieved efficiency in the performance of the public function, lower spending and therefore budget to develop additional activities or projects.

Keywords: computer audit, computer control, internal control, internal control system.

I. INTRODUCCIÓN

En el marco de la Constitución Política, y la Ley N° 27785 - Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, en marzo de 2006, el Congreso de la República emitió la Ley N° 28716, Ley del Control Interno de las Entidades del Estado; otorgando a la Contraloría General la facultad de dictar disposiciones para su cumplimiento.

Mediante Resolución de Contraloría N° 320-2006-CG se aprueban la Normas Técnicas de Control Interno, en aplicación de la Ley N° 28716, las mismas que son de aplicación a las entidades del estado.

Posteriormente con Resolución de Contraloría General N° 458-2008-CG, se aprueba la Guía para la Implementación del Sistema Nacional de Control de las Entidades del Estado, estableciéndose un plazo de 24 meses a todas las entidades de Estado; precisando inclusive los informes parciales y finales que materializarán dicho objetivo.

Sin embargo, aun las instituciones del estado peruano no logran este objetivo y por ende, no ejercen una eficiente gestión para la ejecución del presupuesto público; debido a limitaciones legales o al desconocimiento del uso racional y formal de las leyes o reglamentos. Sumado a esto; la carencia de valores de algunos funcionarios; conlleva a que los procedimientos legales no se cumplan y por lo tanto las adquisiciones o contrataciones no sean transparentes o se entrampen, lo que genera malversación de fondos y deficiencias en la gestión; truncando o retrasando obras y/o mejoras de los servicios públicos, en perjuicio de la sociedad.

A finales del siglo pasado nace el control como una función gerencial, para asegurar y constatar que los planes y políticas preestablecidas se cumplan tal como fueron fijadas; para

lo cual, los contadores idearon la comprobación interna, conocida como: "la organización y coordinación del sistema de contabilidad y los procesos adoptados, que tienen como finalidad brindar a la administración, hasta donde sea posible, práctico y económico, el máximo de protección, control e información verídica". (Rivero y Campos, 2011).

Con esta finalidad, a nivel mundial, se han publicado diversos modelos de control, así como numerosos lineamientos para un mejor gobierno corporativo; siendo los modelos COSO y COCO son de mayor aplicación en el mundo. Su importancia radica en que permiten a la gerencia hacer frente a la rápida evolución del entorno económico y competitivo, así como a las exigencias y prioridades cambiantes de los clientes, adaptando su estructura para asegurar el crecimiento futuro. (Rivas, 2011)

El Sistema Nacional de Control del estado peruano está conformado por: la Contraloría General de República (CGR), que es la cabeza del sistema como ente técnico rector del mismo, las Oficinas de Control Institucional (OCI), como unidades orgánicas responsables de la función de control gubernamental en cada entidad pública y las Sociedades de Auditoria (SOA); que son empresas privadas que, por encargo de la Contraloría General de la República, realizan auditorias financieras, de gestión y exámenes especiales, las cuales comprenden además la ejecución de auditorías a su sistema informático.

La Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, establece que “El control interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúe correcta y eficientemente, siendo responsabilidad del Titular de la entidad fomentar y supervisar el funcionamiento y confiabilidad del control interno para la evaluación de la gestión y el

efectivo ejercicio de la rendición de cuentas, propendiendo a que éste contribuya con el logro de la misión y objetivos de la entidad a su cargo".

Sin embargo; las autoridades del estado no hacen uso eficiente de los recursos públicos por temor a ser denunciados por tomar decisiones no contempladas en los reglamentos, por desconocer los procedimientos a seguir y no contar con sistemas informáticos adecuados que les permita conocer el estado situacional y correcto de la gestión, sirva para efectuar un control eficiente y eficaz y les ayude en la toma de decisiones. (Castello, 1998).

Nuestra experiencia de más de 20 años como Especialistas de las Sociedades de Auditoría Externa en auditoría al sistema informático, en un principio y Expertos, después; nos ha permitido obtener data abundante sobre el estado situacional de varias Oficinas de Informática de diversas entidades del estado peruano, lo cual ha servido de evidencia para observar el nulo o reducido avance en la gestión, año tras años y ha motivado la necesidad de diseñar un sistema que sirva de apoyo a los funcionarios para que el gerenciamiento de las tecnologías de información mejore de manera continua, de tal manera que se puedan desarrollar de forma más rápida, eficiente y oportuna las auditoría de control.

El Objetivos de este estudio es brindar una herramienta de gestión para optimizar el sistema informático de las entidades públicas, mediante la implementación de una metodología dura que permita mejorar la infraestructura de las oficinas de TI a través de la mejora continua de los procesos de adquisición, uso y mantenimiento de los recursos de TI e implementación de normas de seguridad informática; con lo cual se mejorará la gestión y por ende las auditorias de control.

1.1. Planteamiento del problema

La situación de que las instituciones del estado peruano no ejerzan una eficiente gestión para la ejecución del presupuesto público debido a limitaciones legales o al desconocimiento del uso racional y formal de las leyes o reglamentos, sumado a esto la carencia de valores de algunos funcionarios; conlleva a que los procedimientos legales no se cumplan y por lo tanto las adquisiciones o contrataciones no sean transparentes o se entrampen, lo que genera malversación de fondos y deficiencias en la gestión; truncando o retrasando obras y/o mejoras de los servicios públicos y perjudicando, de esta manera, a la sociedad.

En otras situaciones las autoridades no hacen uso eficiente de los recursos públicos por temor a ser denunciados, al no disponer o desconocer procedimientos a seguir, y tomar decisiones no contempladas en los reglamentos, y menos aún no contar con sistemas informáticos adecuados que le ayuden en la toma de decisiones y a la vez disponer de la información basado en computadoras que le permita conocer el estado situacional y correcto de la gestión y por otro lado sirva de un control eficiente y eficaz para la Oficina de Control Interno; tales limitaciones en algunos casos generan que no se realicen inversiones o gastos por problemas presentados en la no previsión dentro de los proyectos. Por otro lado existen gastos en procesos oscuros que salen del procedimiento o alteran los procesos de manera fraudulenta.

1.2. Descripción del problema

En el marco de la Constitución Política, y la Ley N° 27785 (Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República), en marzo de 2006, el Congreso de la República emite la Ley N° 28716, Ley del Control Interno de las Entidades

del Estado; otorgando a la Contraloría General la facultad de dictar disposiciones para su cumplimiento.

Mediante Resolución de Contraloría N° 320-2006-CG se aprueban la Normas Técnicas de Control Interno, en aplicación de la Ley N° 28716, las mismas que son de aplicación a las entidades del estado.

Posteriormente con Resolución de Contraloría general N° 458-2008-CG, se aprueba la Guía para la Implementación del Sistema Nacional de Control de las Entidades del Estado, estableciéndose un plazo de 24 meses a todas las entidades de Estado. Precisando inclusive los informes parciales y finales que materializarán dicho objetivo.

Estamos en el segundo semestre de 2019 y dicho objetivo es aún lejano dado el estado situacional de tal obligación legal.

Nuestra experiencia de más de 20 años como Especialistas de las Sociedades de Auditoría Externa en auditoría al sistema informático, en un principio y Expertos, después; nos ha permitido obtener data abundante sobre el estado situacional de varias Oficinas de Informática de diversas entidades del estado peruano, lo cual ha servido de evidencia para observar el nulo o reducido avance en la gestión, año tras años y ha motivado la necesidad de diseñar un sistema que sirva de apoyo a los funcionarios para que el gerenciamiento de las tecnologías de información mejore de manera continua, de tal manera que se puedan desarrollar de forma más rápida, eficiente y oportuna las auditoría de control.

El Objetivos de este estudio es: Optimizar el sistema informático, mediante la implementación de una metodología dura que permita mejorar la infraestructura de las oficinas de TI a través de la mejora continua de los procesos de adquisición, uso y

mantenimiento de los recursos de TI e implementación de normas de seguridad informática; con lo cual se mejorará la gestión y por ende las auditorias de control.

1.3. Formulación del problema

1.3.1. *Problema general*

¿Cómo la implementación de una metodología para optimizar la gestión del sistema informático mejoraría la ejecución del gasto en una entidad del sector público sujeta al sistema nacional de control interno?

1.3.2. *Problemas* específicos.

- ¿La organización e infraestructura de las oficinas de TI mediante la implementación de una metodología contribuirá en alcanzar los objetivos y metas del Control Interno?

- ¿Las adquisiciones, uso y mantenimiento de los recursos de TI mediante la implementación de una metodología, mejorarán la gestión de la entidad?

- ¿El hardware y software instalado mediante la implementación de una metodología cumplirá con las normas de Seguridad Informática?

1.4. Antecedentes

1.4.1. A nivel internacional

A finales del siglo pasado, como consecuencia del notable aumento de la producción, los propietarios de los negocios se vieron imposibilitados de continuar atendiendo personalmente los problemas productivos, comerciales y administrativos, viéndose forzados a delegar funciones dentro de la organización conjuntamente con la creación de sistemas y procedimientos que previeran o disminuyeran fraudes o errores, debido a esto comenzó a hacerse sentir la necesidad de llevar a cabo un control sobre la gestión de los negocios, ya que se había prestado más atención a la etapa de producción y comercialización que a la administrativa u organizativa, reconociéndose la necesidad de crear e implementar sistemas de control como consecuencia del importante crecimiento operado dentro de las entidades. Así nace el control como una función gerencial, para asegurar y constatar que los planes y políticas preestablecidas se cumplan tal como fueron fijadas.

Debido a esto los contadores idearon la comprobación interna, la cual era conocida como: "la organización y coordinación del sistema de contabilidad y los procesos adoptados, que tienen como finalidad brindar a la administración, hasta donde sea posible, práctico y económico, el máximo de protección, control e información verídica".

El término de Control Interno reemplazó al de comprobación interna, debido a un cambio conceptual, ya que el contenido del mismo ha sufrido una considerable evolución.

Se puede afirmar que el Control Interno ha sido preocupación de la mayoría de las entidades, aunque con diferentes enfoques y terminologías, lo cual se puede evidenciar al consultar los libros de texto de auditoría, los artículos publicados por organizaciones profesionales, universidades y autores individuales (Riveros, 2011).

A partir de la divulgación del COSO se ha publicado diversos modelos de control así como numerosos lineamientos para un mejor gobierno corporativo; siendo los más conocidos el COCO (USA), el COCO (Canadá), el CADBURY (Reino Unido), el VIENOT (Francia), e PETERS (Holanda), y King (Sudáfrica); entre otros. Los modelos COCO y COSO son de mayor aplicación en el mundo. "Su importancia radica en que permiten a la gerencia hacer frente a la rápida evolución del entorno económico y competitivo, así como a las exigencias y prioridades cambiantes de los clientes, adaptando su estructura para asegurar el crecimiento futuro.

En resumen existen diferentes estructuras conceptuales, pero en el mercado de capitales de los Estados Unidos de Norteamérica al que se reconoce como criterio de control es el COSO. Este se consolida como el punto de partida para importantes desarrollos en las áreas del control interno de los nuevos instrumentos financieros, gubernamental y sistemas de información, y anuncia una nueva orientación a la dirección de una organización que es la administración de sus riesgo e implica una comprensión de la organización en términos de sistemas, que por ende orienta a entender el significado de los diferentes elementos que la conforman y su relación en función a los objetivos que esta persigue.

Modelos Contemporáneos de Control Interno: Fundamentos Teóricos A partir de la década de los noventa, los nuevos modelos desarrollados en el campo del control están definiendo una nueva corriente de pensamiento, con una amplia concepción sobre la organización, involucrando una mayor participación de la dirección, gerentes y personal en general de las organizaciones a nivel mundial. Estos modelos han sido desarrollados con la idea de que representen fuertes soportes del éxito de la organización, siempre que los mismos sean llevados con el criterio y la perspicacia necesaria de parte del profesional. Se han publicado diversos modelos de Control, así como numerosos lineamientos para un mejor gobierno corporativo. Los modelos más conocidos son: el COSO (USA), el COCO (Canadá),

el CADBURY (Reino Unido), el VIENOT (Francia), el PETERS (Holanda), KING (Sudáfrica) y MICIL (adaptación del COSO para Latinoamérica). Los modelos COSO, COCO y MICIL son los más adoptados en las empresas del continente americano; es por ello que el análisis de los fundamentos teóricos de los modelos contemporáneos de control interno que se presenta a continuación centra su atención en los mismos.

Se inicia el recorrido en el denominado informe COSO (Committee of Sponsoring organizations) comisionado por los cinco organismos profesionales financieros más importantes de los Estados Unidos, fue definido en 1992; tras cinco años de estudio y discusión, surge un nuevo marco conceptual del control interno con el objetivo fundamental de integrar las diversas definiciones y conceptos vigentes para este momento. A nivel organizacional, se realza la necesidad de que la alta dirección y el resto de la organización comprendan cabalmente la trascendencia del control interno, la incidencia del mismo sobre los resultados de su gestión, el papel estratégico a conceder a la auditoría y esencialmente la consideración del control como un proceso integrado a las operaciones de la empresa y no como un conjunto de reglas A nivel normativo, pretende plantear y normas rígidas, compuesto por mecanismos burocráticos. Una referencia conceptual común a nivel de auditoría interna, externa, en los ámbitos académicos o legislativos, lo cual hasta ahora resultaba complejo, dada la multiplicidad de definiciones y conceptos divergentes que han existido sobre control interno. De acuerdo al marco integrado de control interno COSO (Modelo COSO), el control interno consta de cinco categorías o componentes que la administración diseña y aplica para proporcionar una seguridad razonable de que sus objetivos de control se llevaran a cabo de manera adecuada. Estos componentes son: (1) Ambiente de Control; (2) Evaluación de los Riesgos; (3) Actividades de Control; (4) Información Y comunicación; y (5) Monitoreo. Por desempeñarse en una base de tiempo real reaccionan dinámicamente a las condiciones cambiantes y están integrados a la gestión de la organización, proporcionan una

retroalimentación sobre la efectividad de los otros componentes de control interno. Se realizan evaluaciones separadas que son necesarias para que la administración tenga una seguridad razonable respecto de la efectividad del sistema de control interno, se realizan cada cierto tiempo. Para este tipo de evaluación se debe tener presente: a) el alcance y frecuencia de la evaluación; b) el proceso de evaluación; c) La metodología de evaluación; y; d) el nivel de documentación.

El siguiente modelo a considerar es el denominado "Modelo COCO (Criteria of Control)" de Canadá, es producto de una profunda revisión realizada por el Comité de Criterios de Control de Canadá sobre el reporte COSO, el propósito de esta revisión se centró en hacer el planteamiento de un Modelo más sencillo y comprensible, ante las dificultades que en la aplicación del COSO enfrentaron inicialmente algunas organizaciones".

El modelo COCO (Criteria of Control) de Canadá, fue publicado tres años más tarde que COSO; éste simplifica los conceptos y el lenguaje para hacer posible una discusión sobre el alcance total del control, con la misma facilidad en cualquier nivel de la organización empleando un lenguaje más sencillo, para hacerle accesible para todos los empleados de una empresa. El cambio importante que plantea el Modelo Canadiense consiste que, en lugar de conceptualizar al proceso de Control como una pirámide de componentes y elementos interrelacionados, proporciona un marco de referencia a través de 20 criterios generales, que el personal en toda la organización puede usar para diseñar, desarrollar, modificar o evaluar el Control. Las organizaciones que pretendan aplicar los lineamientos de COCO, deberán tener un claro conocimiento y consideración de los cinco componentes que conforman el marco integrado de control interno publicado por COSO. La estructura del modelo canadiense requiere de creatividad para su interpretación y aplicación, y es adaptable a cualquier organización una vez que se adecua a las necesidades de sus propios intereses, o usarlas de referencia para desarrollar un modelo propio. En este orden de ideas Estupiñán expone

(2006:10), el modelo COCO "busca proporcionar un entendimiento del control y dar respuesta a las tendencias que se observan en los desarrollos siguientes: - El impacto de la tecnología y el recorte a las estructuras organizacionales, que han proporcionado mayor énfasis sobre el control a través de medios informales, como la visión empresarial compartida, comunión de valores y una comunicación abierta; -En la creciente demanda de informar públicamente acerca de la efectividad del control, respecto a ciertos objetivos; - En el énfasis de las autoridades para establecer controles, como una forma de proteger los intereses de los accionistas. Algunas autoridades financieras han establecido procedimientos y protocolos de información, aplicables a las instituciones bajo su jurisdicción". (Rivas, 2016)

1.4.2. *A nivel nacional*

El Sistema Nacional de Control de la República del Perú es el conjunto de órganos, instituciones, normas, métodos y procedimientos que permiten conducir y desarrollar las actividades de control del Estado en el Perú de manera descentralizada. Está regulada por la Ley Nº 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.

El Sistema Nacional de Control está conformado por:

- La Contraloría General de República (CGR), que es la cabeza del sistema como ente técnico rector del mismo.
- Las Oficinas de Control Institucional (OCI), como unidades orgánicas responsables de la función de control gubernamental en cada entidad pública.
- Las Sociedades de Auditoria (SOA); que son empresas privadas que, por encargo de la Contraloría General de la República, realizan auditorias financieras, de gestión y exámenes especiales, las cuales comprenden además la ejecución de auditorías a su sistema informático.

Mediante el artículo 6° de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, establece que el control gubernamental consiste en la supervisión, vigilancia y verificación de los actos y resultados de la gestión pública, en atención al grado de eficiencia, eficacia, transparencia y economía en el uso y destino de los recursos y bienes del Estado, así como del cumplimiento de las normas legales y de los lineamientos de política y planes de acción, evaluando los sistemas de administración, gerencia y control, con fines de su mejoramiento a través de la adopción de acciones preventivas y correctivas pertinentes.

Asimismo en el artículo 7° de la citada Ley, establece que el control interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúe correcta y eficientemente, siendo responsabilidad del Titular de la entidad fomentar y supervisar el funcionamiento y confiabilidad del control interno para la evaluación de la gestión y el efectivo ejercicio de la rendición de cuentas, propendiendo a que éste contribuya con el logro de la misión y objetivos de la entidad a su cargo.

En este marco, la Ley N° 28716, Ley de Control Interno de las Entidades del Estado, establece que la Contraloría General de la República es la entidad competente para dictar la normativa técnica de control que oriente la efectiva implantación y funcionamiento del control interno en las entidades del Estado, así como su respectiva evaluación; que, la Resolución de Contraloría N° 458-2006-CG, que aprobó la "Guía para la Implementación del Sistema de Control Interno de las entidades del Estado" con el objetivo principal de proveer de lineamientos, herramientas y métodos a las entidades del Estado para la implementación de los componentes que conforman el Sistema de Control Interno (SCI) establecido en las Normas de Control Interno (NCI); que, la Ley N° 30372, Ley del Presupuesto del Sector Público para el Año Fiscal 2016, en su Quincuagésima Tercera Disposición Complementaria Final, establece la

obligación de todas las entidades de los tres niveles de gobierno de implementar su Sistema de Control Interno, en un plazo máximo de treinta y seis (36) meses, contados a partir de su entrada en vigencia; para lo cual la Contraloría General de la República emitirá las disposiciones conteniendo los plazos por cada fase y nivel de gobierno y los demás lineamientos que sean necesarios.

En este contexto emitió la Directiva N.° 013-2016-CG/GPROD denominada "Implementación del Sistema de Control Interno (SCI) en las Entidades del Estado", aprobada por Resolución de Contraloría N° 149-2016-CG, que regulaba el nuevo modelo y los nuevos plazos para la implementación del Sistema de Control Interno que deben realizar las entidades del Estado en los tres niveles de gobierno. Estos modelos y plazos fueron postergados por sendas Resoluciones de Contraloría. Siendo la última la Nº 095-2022-CG del 7 de marzo de 2022, que dispone que la implementación del SCI en las entidades del estado peruano entrarán en vigencia a partir del año 2023.

Así mismo; mediante Resolución de Contraloría Nº 445-2014-CG, se aprueba un nuevo Manual de Auditoría Financiera Gubernamental, que comprende, entre otros aspectos, lineamientos para auditar las Oficinas de Informática, en el marco del control interno.

1.5. Justificación de la investigación

La auditoría en informática o de tecnologías de la información (TI) es de vital importancia para el buen desempeño de los sistemas informáticos, debido a que proporciona los controles necesarios para que los resultados sean oportunos, confiables y seguros. Se establece tres tipos de funciones para los auditores de TI:

- Revisar y evaluar el diseño, elaboración, implantación y explotación de las aplicaciones informáticas en las instituciones del estado.
- Revisar y evaluar los controles implementados en los sistemas informáticos.

- Revisar y evaluar la eficacia, utilidad, fiabilidad y seguridad de los equipos y programas informáticos implementados en las instituciones del estado.

1.5.1. *Justificación teórica*

La necesidad de contar con una información veraz, actualizada, y oportuna, que sirva de base para tomar decisiones en las entidades del sector público, a fin de lograr el cumplimiento de normas, leyes y otras disposiciones que permitan mejorar y hacer más eficiente la organización de las entidades y que se promueva la implementación de mejores prácticas. Por lo que el presente trabajo, toma en consideración la importancia que tiene el proceso de control interno en la organización pública, con el fin de obtener mejor resultados.

1.5.2. *Justificación práctica*

Nos permitirá ingresar a la parte álgida o columna vertebral de las entidades, porque cuando no existe un proceso o sistema de control adecuado, los recursos públicos se exponen a la presencia de errores y fraudes de los recursos en general, generando en consecuencia la implantación de malas prácticas y deterioro de una cultura organizacional.

1.5.3. *Justificación metodológica*

La investigación se inicia recopilando datos de la problemática existente en las diversas instituciones del estado, información estadística obtenida por la Gerencia de Control Interno de la Contraloría General afín de medir el grado de promoción e implementación del control interno en base a la aplicación de la Ley N° 28716 y a partir del análisis plantear alternativas de solución que mejore el desenvolvimiento de las responsables de la administración del presupuesto público.

1.5.4. *Justificación social*

El proceso de auditoria informática como parte del control interno es de vital importancia para un mejor eficiencia y eficacia de la gestión de entidades del sector público en cuanto al uso y gasto de los recursos presupuestados anualmente para la adquisición de bienes,

ejecución de obras y prestación de servicios, por lo cual la investigación tiende a reducir o encauzar de manera correcta, oportuna y veraz la información referente al gasto público proveniente del Presupuesto General de la República.

1.5.5. *Importancia de la investigación*.

La implementación de una metodología para la gestión de auditoria informática en el Control Interno bajo el concepto COSO 1 y los conceptos que actualizan su prescripción reviste importancia no solo por la obligación legal, si no por la necesidad pragmática de lograr un estado eficiente que cumpla con las mínimas exigencias de bienestar para la población en general.

La presente investigación servirá de base para ir mejorando la gestión y para futuras investigaciones en el marco de desarrollo de la Contraloría General de la Republica, servirá además de referencia para los investigadores en este sector provenientes de las escuelas de Post Grado.

1.5.6. *Fundamento*.

La implementación del Sistema de Control Interno en aplicación de la Ley N.° 28715, es una obligación legal y una necesidad institucional, sin embargo los extremos relacionados a sus componentes constituyen una problemática por el estado situacional del sector público, por lo que induce a mejorar el sistema y su aplicabilidad.

Con la presente investigación se inducirá a mejorar el uso de los recursos presupuestados y el control de los mismos, encausando a la entidad hacia una gestión eficiente y eficaz para el bienestar de la sociedad.

1.6. Limitaciones de la investigación

1.6.1. *Espacial*

El trabajo de investigación se desarrolla en la ciudad de Lima tomando como referencia las entidades del sector público de orden nacional.

1.6.2. *Temporal*

El trabajo de investigación tiene una duración de once meses, desde septiembre 2018 hasta agosto 2019. Se toma como referencia la recolección de datos e información de los últimos 05 años (2013 al 2017).

1.6.3. *Social*

Comprende a todos los actores que intervienen directa ó indirectamente en el trabajo de investigación y esta conformado por las entidades del gobierno nacional y gobierno regional:

- Congreso de la República - CG
- Consejo Nacional de la Magistratura - CNM
- Contraloría General de la República - CGR
- Defensoría del Pueblo - DP
- Jurado Nacional de Elecciones - JNE
- Ministerio de Agricultura - MINAG
- Ministerio de Comercio Exterior y Turismo - MINCETUR
- Ministerio de Defensa - MINDEF
- Ministerio de Economía y Finanzas - MEF
- Ministerio de Educación - MINEDU
- Ministerio de Energía y Minas - MEM
- Ministerio de Justicia - MJ

- Ministerio de la Mujer y Desarrollo Social - MIMDES
- Ministerio de la Producción - PRODUCE
- Ministerio de Relaciones Exteriores - MRREE
- Ministerio de Salud - MINSA
- Ministerio de Trabajo y Promoción del Empleo - MTPE
- Ministerio de Transportes y Comunicaciones - MTC
- Ministerio de Vivienda, Const. y Saneamiento - MIVCS
- Ministerio del Ambiente - MINAM
- Ministerio del Interior - MININTER
- Ministerio Público - MP
- Oficina Nacional de Procesos Electorales - ONPE
- Poder Judicial - PJ
- Presidencia del Consejo de Ministros - PCM
- Registro Nacional de Identificación y Estado Civil - RENIEC
- Tribunal Constitucional - TC
- Superintendencia Nacional de Administración Tributaria
- Dirección Nacional del Endeudamiento Público-NEP (CAP.)
- Instituciones descentralizadas
- Universidades
- Organismos descentralizados autónomos
- Gobiernos regionales

1.7. Objetivos

1.7.1. *Objetivo general*

Optimizar el sistema informático para hacer más eficaces las auditorias de control interno mediante la implementación de una metodología dura en las entidades públicas sujetas al Sistema Nacional de Control.

1.7.2. Objetivos específicos

- Contribuir en alcanzar objetivos y metas del Control Interno, mediante la implementación de una metodología, mejorando la gestión e infraestructura de las oficinas de TI.
- Mejorar los procesos de adquisición, uso y mantenimiento de los recursos de TI, mediante la implementación de una metodología dura para las entidades públicas sujetas al Sistema Nacional de Control.
- Implementar normas de seguridad informática para el software y hardware; mediante la implementación de una metodología dura.

1.8. Hipótesis y variables

1.8.1. *Hipótesis principal*.

La implementación de una metodología dura para optimizar el sistema informático en las entidades públicas; mejoraría el control interno y por ende; el uso de los recursos.

1.8.2. *Hipótesis secundarias*.

- La mejora de la organización e infraestructura de las oficinas de TI mediante la implementación de una metodología dura contribuiría en alcanzar los objetivos y metas del Control interno.
- Las adquisiciones, uso y mantenimiento de los recursos de TI, con la implementación de una metodología, mejoraría la gestión de la entidad pública.
- El hardware y software instalado mediante la implementación de una metodología dura cumpliría con las normas de seguridad Informática.

1.8.3. *Variables*.

a) Hipótesis Principal

VI: Metodología para mejorar la gestión informática.

VD: Mejorar el control interno.

Eficacia en el uso de los recursos.

b) Hipótesis Secundarias

1) VI: Organización e infraestructura de la oficina de TI.

VD: Gestión, objetivos y metas.

2) VI: Gestión informática.

VD: Eficiencia en:

- Adquisición de hardware y software.
- Uso de hardware y software.
- Mantenimiento de hardware y software.

3) VI: Hardware y software.

VD: Seguridad informática.

II. MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Desde cuando existe el problema

El control previo y concurrente compete exclusivamente a las autoridades, funcionarios y servidores de las entidades, el cual es ejercido según lo estipulado en sus Reglamentos y Manuales de Organización y Funciones (ROF y MOF); Manuales de Procedimientos y Reglamentos Internos de Trabajo, entre otros, los mismos son formulados y aprobados por las autoridades y funcionarios de las propias entidades , generando la heterogeneidad en todo el sector público del contenido de estas normas, como: obligaciones y responsabilidades de todo el personal de la institución, empezando desde el titular; su funciones, delimitaciones de labores, controles previos y concurrentes, entre otros, que son los que coadyuvan a que la administración opere dentro de las normas y tendiendo al logro de objetivos y cumplimiento de metas institucionales.

Esta heterogeneidad, tiene como una de sus causas la ausencia de normas específicas relacionadas a uniformizar conceptos y formulación de normativa de gestión, toda vez que la institución que lo hacía dejó de operar desde el año 1990, esta organización denominada Instituto Nacional de Administración Pública - INAP, si bien es cierto dejó sus normas vigentes, estas provenían desde el año 1982, lo cual como es lógico, a la fecha han devenido en inoportunas e ineficaces, debido al cambio de tendencias, mejoras en la doctrina administrativa y en los cambios del aparato gubernamental, el cual en estos momentos de globalización, de alta dependencia de los sistemas informáticos, que se tiende a la descentralización y por consiguiente se requiere de nuevas herramientas de gestión y de control.

En este orden, la idea principal es señalar que el control interno tiende a lograr la unificación de criterios y conceptos normativos, sobre todo si tenemos en cuenta que es una de

las maneras como debe aplicarse el control gubernamental. el cual se da mediante la aplicación de principios, sistemas y procedimientos, tal como se deja entender en el artículo segundo de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General.

Otro de los escenarios proclives de deficiencias en la administración Publica son los gobiernos locales, toda vez que son pocas las municipalidades que cuentan con manuales o reglamentos que precisen las funciones de su personal y las responsabilidades o sanciones a que se harían merecedores si las incumplen, de tal manera que en muchos casos quien decide, el destino y uso de los recursos de la municipalidad es el alcalde o los superiores jerárquicos, con la complacencia de los mandos intermedios; ante esta situación, urge que se den alternativas de control interno y de eficiencia de gestión y que las acciones a seguir deben ser de obligatorio cumplimiento y sancionado el que las incumpla, asimismo se respalde el accionar correcto de los servidores de mando medio en la gestión pública y se sienta respaldados con procedimientos legales que eviten ser presionados para acceder a las disposiciones negativas de sus superiores inmediatos.

Se debe recordar que, las normas que rigen las actividades de la organización señaladas en el artículo T" de la Ley N° 27785, no tienen fuerza de ley y no precisan uniformidad en el sector público, de tal manera que algunos señalan en los niveles superiores la responsabilidad y en otros quien asume ésta es el nivel medio; las municipalidades por ejemplo, no obstante que su ley orgánica señala que el alcalde es responsable de sus actos, este delega muchas veces sus acciones negativas en sus subordinados, con lo cual no es pasivo de sanción.

Por todos en sabido que, los gobiernos a través de funcionarios corruptos institucionalizan la corrupción, de tal manera que se puede encontrar como lapidan fondos del Estado en pagar coimas, adquieren bienes sobrevaluados, gastos superfluos, planillas doradas no legales, pago de gastos personales o particulares, retiro de fondos sin el sustento adecuado ni formal, nombramientos de funcionarios y servidores públicos sin someterse a la normativa,

entre otros asuntos que se van revelando poco a poco, mediante las investigaciones de las instancias competentes como Contraloría General de la República, Ministerio Público, Congreso de la República, entre otras.

Todos estos actos irregulares, delictivos, tienen un costo de miles de millones de dólares, el cual según versiones de las Procuradurías los actos de corrupción de malos funcionarios de los Gobiernos de Fujimori, de Toledo y de García se estiman en miles de millones de soles, fondos que van a parar a las manos o cuentas secretas abiertas en el extranjero, por los testaferros o por los mismos participantes del circulo corrupto gubernamental.

Efecto de la vigencia de la norma sobre la legislación nacional:

En lo que respecta al "Sistema Nacional de Control", está normado por la Ley N° 27785, y el proyecto de la Ley de Control Interno, no era antagónico, por el contrario es coadyuvante y complementario al control previo y concurrente que ejecutan los funcionarios y servidores públicos.

Respecto a la normativa emitida por el ex Instituto Nacional de Administración Pública-INAP, estas fueron dadas mediante resoluciones Jefaturales, en el año 1982, siendo que a la fecha siguen vigentes por la fuerza de la costumbre, mas están desactualizadas al haber cambios bastante marcados en la administración pública no solo a nivel nacional sino internacionalmente, y por el avance tecnológico tenemos: rapidez de las comunicaciones, mejora de los equipos informáticos, cambios en la estructura del Estado. Por lo que es necesario un aporte al desarrollo de las actividades de la Contraloría General de la República.

En el segundo párrafo del Artículo Segundo (RC N° 458-2008-CG), se establece un plazo máximo de veinticuatro (24) meses para la implementación del Sistema de Control Interno a partir del día siguiente de publicada la presente Resolución.

Sin embargo, en forma posterior el Estado se dispone modificar el Art. 10° de la Lev N° 28716, incorporando como cuarto párrafo del artículo en mención, lo siguiente:

"El marco normativo y la normatividad técnica de control que dicte la Contraloría General de la República a que se refiere el párrafo anterior serán de aplicación progresiva, teniendo en cuenta la naturaleza de las funciones de las entidades, así como la disponibilidad de recursos presupuestarios, debiendo entrar en vigencia cuando se culmine la aprobación de todas las Leyes de Organización y Funciones de los diversos Sectores de Gobierno Nacional y de sus respectivos documentos de gestión, así como cuando el SIAF SP versión 1/, el cual incluirá el módulo de evaluación de Control Interno, esté implementado en los tres niveles de gobierno".

Consecuentemente quedaban sin efecto los plazos establecidos, más no la obligación de adecuar el SCI, a las disposiciones dictadas.

Posteriormente, mediante Ley 29743 se modifica el Art. 10° de la Ley N° 28716", sustituyendo el cuarto párrafo del artículo en mención, por el siguiente texto:

"El marco normativo y la normativa técnica de control que emite la Contraloría General de la República en el proceso de implantación del SCI, toma en cuenta la naturaleza de las funciones de las entidades, proyectos de inversión, actividades y programas sociales que estas administran".

Muy independientemente a lo señalado en estos dos últimos dispositivos (Decreto de Urgencia N° 067-2009 y la Ley N° 29743), ésta vigente lo señalado en el cuarto párrafo de la Ley N° 27785, tercer párrafo del Artículo 4° de la Ley N° 28716, y el Artículo 6° de la Ley N° 28716. Tener en cuenta lo señalado en el Artículo 8° de la Ley N° 28716 que señala textualmente lo siguiente:

"La inobservancia de la presente Ley, genera responsabilidad administrativa funcional, y da lugar a la imposición de la sanción de acuerdo a la normativa aplicable, sin perjuicio de la responsabilidad civil o penal a que hubiere lugar, de ser el caso".

2.2. Bases teóricas

2.2.1. Administración pública

Es el servicio de los ciudadanos y ciudadanas y se fundamenta en los principios de honestidad, participación, celeridad, eficiencia, transparencia, rendición de cuentas y responsabilidad en el ejercicio de la función pública, con sometimiento pleno a la ley y al derecho"

Podemos definir la Administración Pública como el contenido esencial de la actividad del Estado, y se refiere a las actividades de gestión, que el titular de la misma y sus colaboradores desempeñan sobre los recursos del Estado para suministrarlos de forma inmediata y permanente, a la satisfacción de las necesidades y lograr con ello el bien general, dicha atribución tiende a la realización de un servicio público, y se somete al marco jurídico especializado que norma su ejercicio y se concretiza mediante la emisión y realización

2.2.2. Estructura del Estado Peruano

Poder Ejecutivo:

Es el órgano autónomo encargado de hacer cumplir y ejecutar las leyes, así también responsable del buen funcionamiento de los servicios públicos. Está conformado por el Presidente de la República, los vice presidentes y los ministros del Estado.

El presidente de la República es el jefe del Estado y personifica a la Nación. Es elegido en sufragio directo por un periodo de cinco años. Las atribuciones más importantes del Presidente de la República son:

- Cumplir y hacer cumplir la constitución, los tratados, leyes y demás disposiciones legales.
- Representar al Estado, dentro y fuera de la república.
- Dirigir la política general de gobierno.
- Velar por el orden interno y la seguridad exterior de la República.
- Convocar a elecciones.
- Conceder indultos y conmutar penas.
- Convocar al congreso a legislatura extraordinaria.
- Otros señalados en la Constitución Art. 110 – 118.

El Consejo de Ministros.- Órgano del poder ejecutivo integrado por la reunión de ministros encargados de la conducción de los diversos sectores públicos. Cada ministerio es el responsable de la dirección y gestión de los asuntos que competen a la cartera a su cargo.

El presidente del Consejo de Ministros, quien puede ser ministro sin cartera, es, después del Presidente de la República, el portavoz autorizado del gobierno, coordina las funciones de los ministerios y firma los decretos legislativos, los decretos de urgencia y resoluciones que señala la ley y la constitución.

Poder Legislativo.

Órgano del Estado encargado de dictar, modificar y derogar las leyes. También tiene atribuciones de fiscalización con respecto a las instituciones y a los funcionarios que las ejercen a través de comisiones investigadoras.

El Congreso de la República es la expresión del poder legislativo. Está integrado por cámara única compuesta por 130 representantes, elegidos por cinco años mediante voto electoral directo, secreto y obligatorio. Los requisitos para ser congresistas, las funciones, atribuciones y otros están en la Constitución Art. 90 – 102.

El Congreso de la República está organizado por: la Comisión Permanente, las Comisiones Investigadoras y las Comisiones Dictaminadoras.

Poder Judicial.

Poder del Estado, que tiene autonomía política, administrativa, económica, disciplinaria e independiente en lo jurisdiccional. Encargado de administrar justicia, conforme a la constitución y las leyes, a las personas e instituciones que conforman la sociedad.

Principios y derechos de la función jurisdiccional: implica que el Poder Judicial a través de sus órganos jurisdiccionales, es el único llamado a administrar justicia en todo el territorio nacional, excepto la extensión jurisdiccional y el derecho consuetudinario.

Sus funciones, atribuciones y demás están en los artículos 138 – 149 de la Constitución.

2.2.3. Presupuesto nacional, aprobación y procedimientos.

Los Estados, perciben un conjunto de ingresos por su capacidad coercitiva de cobrar tributos. Estos ingresos se transforman en gastos, que deben aplicarse de la forma más eficaz y eficiente posible, de modo que se traduzca en servicios públicos cada vez mejores a la comunidad. En ese marco, el presupuesto público es una herramienta fundamental de la gestión de las finanzas que sirve como elemento básico para lograr los objetivos contenidos en los planes gubernamentales, financiando las actividades y proyectos contenidos en estos. En base a las políticas y objetivos gubernamentales, la prioridad al gasto, en países como el Perú, debe atender el gasto social con criterios de calidad y equidad, el gasto de inversión para generar condiciones favorables a la competitividad, sobre la base de mejorar del capital físico y humano del país, para que en el mediano plazo se refleje en un mayor crecimiento, inversión, empleo, así como el mejor aprovechamiento de las oportunidades de desarrollo, de manera que aporte a una economía que compita en el mundo global. Desde el año 2008, se dispone la

implementación progresiva del presupuesto por resultados (PPR) a nivel de programas pilotos para alcanzar objetivos específicos relacionados a la política económica y social.

El Presupuesto comprende: i) Los gastos que, como máximo, pueden contraer las Entidades durante el año fiscal, en función a los créditos presupuestarios aprobados y los ingresos que financian dichas obligaciones, y ii) Los objetivos y metas a alcanzar en el año fiscal por cada una de las Entidades con los créditos presupuestarios que el respectivo presupuesto les aprueba.

La gestión presupuestaria del estado se rige por un conjunto de principios que de dan coherencia y sostenibilidad; aquí se presenta los más importantes: • Equilibrio presupuestario. El Presupuesto del Sector Público está constituido por los créditos presupuestarios que representan el equilibrio entre la previsible evolución de los ingresos y los recursos a asignar, de conformidad con las políticas de gasto, estando prohibido incluir autorizaciones de gasto sin el financiamiento correspondiente. • Equilibrio macro fiscal. La preparación, aprobación y ejecución de los presupuestos de las Entidades preservan la estabilidad conforme al marco de equilibrio macrofiscal. • Especialidad cuantitativa. Toda disposición o acto que implique la realización de gastos públicos debe cuantificar su efecto (costo versus resultado) sobre el Presupuesto, de modo que se sujete en forma estricta al crédito presupuestario autorizado a la Entidad. • Especialidad cualitativa. Los créditos presupuestarios aprobados para las Entidades se destinan, exclusivamente, a la finalidad para la que hayan sido autorizados en los Presupuestos del Sector Público, así como en sus modificaciones realizadas. • De no afectación predeterminado. Los fondos públicos de cada una de las Entidades se destinan a financiar solo el conjunto de gastos públicos previstos en los Presupuestos del Sector Público. • Integridad. Los ingresos y los gastos se registran en los Presupuestos por su importe íntegro, salvo las devoluciones de ingresos que se declaren indebidos por la autoridad competente. • Anualidad. El Presupuesto del Sector Público tiene vigencia anual y coincide con el año calendario;

durante dicho periodo se afectan los ingresos percibidos dentro del año fiscal, cualquiera sea la fecha en los que se hayan generado, así como los gastos devengados que se hayan producido con cargo a los respectivos créditos presupuestarios durante el año fiscal. • Eficiencia en la ejecución de los fondos públicos. Las políticas de gasto público vinculadas a los fines del Estado deben establecerse teniendo en cuenta la situación económica-financiera y el cumplimiento de los objetivos de estabilidad macro fiscal, siendo ejecutadas mediante una gestión de los fondos públicos, orientada a resultados con eficiencia, eficacia, economía y calidad. • Centralización normativa y descentralización operativa. El Sistema Nacional del Presupuesto se regula de manera centralizada en lo técnico normativo, correspondiendo a las Entidades el desarrollo del proceso presupuestario. • Transparencia presupuestal. El proceso de asignación y ejecución de los fondos públicos sigue los criterios de transparencia en la gestión presupuestal, difundiendo la información pertinente a la ciudadanía. • Principio de Programación Multianual. El proceso presupuestario debe apoyarse en los resultados de ejercicios anteriores y tomar en cuenta los ejercicios futuros.

Los fondos públicos están conformados por los ingresos, que por diferente concepto, percibe el Estado. Se orientan a la atención de los gastos que genere el cumplimiento de sus fines, independientemente de la fuente de financiamiento de donde provengan. Los fondos se orientan de manera eficiente y con atención a las prioridades establecidas en las políticas en beneficio del desarrollo del país.

2.2.4. Contraloría General de la República

La Contraloría General de la República del Perú es un organismo constitucional autónomo del Estado Peruano encargado de controlar los bienes y recursos públicos del país.

Es el órgano superior del Sistema Nacional de Control, que cautela el uso eficiente, eficaz y económico de los recursos del Perú, la correcta gestión de la deuda pública, así como

la legalidad de la ejecución del presupuesto del sector público y de los actos de las instituciones sujetas a control; coadyuvando al logro de los objetivos del Estado en el desarrollo nacional y bienestar de la sociedad peruana".

La Contraloría General tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental, orientando su accionar al fortalecimiento y transparencia de la gestión de las entidades, la promoción de valores y la responsabilidad de los funcionarios y servidores públicos, así como, contribuir con los Poderes del Estado en la toma de decisiones y con la ciudadanía para su adecuada participación en el control social".

2.2.5. Atribuciones de la Contraloría General de la República

La Constitución Política de 1993 le da las competencias siguientes:

- Presentar anualmente el informe de auditoría practicado a la Cuenta General de la República (Art. 81º).[1]
- Supervisar la legalidad de la ejecución del Presupuesto del Estado, de las operaciones de la deuda pública y de los actos de las instituciones sujetas a control (Art. 82º).[2]
- Realizar el control para que los Fondos destinados a satisfacer los requerimientos logísticos de las Fuerzas Armadas y Policía Nacional se dediquen exclusivamente para ese fin (Art. 170º).[3]
- Control en Gobiernos Regionales y Locales, al determinar que éstas deben rendir cuenta sobre la ejecución de su presupuesto a la Contraloría General (Artículo 199°).[4]
- Facultad de iniciativa legislativa en materia de control (Art. 107º).[5]

La Ley Orgánica – Ley N° 27785 y sus modificatorias establece las siguientes atribuciones:

- Tener acceso en cualquier momento y sin limitación a los registros, documentos e información de las entidades, aun cuando sean secretos; así como requerir información a particulares que mantengan o hayan mantenido relaciones con las entidades; siempre y cuando no violen la libertad individual.

- Ordenar que los órganos del Sistema realicen las acciones de control que a su juicio sean necesarios o ejercer en forma directa el control externo posterior sobre los actos de las entidades.

- Supervisar y garantizar el cumplimiento de las recomendaciones que se deriven de los informes de control emanados de cualquiera de los órganos del Sistema.

- Disponer el inicio de las acciones legales pertinentes en forma inmediata, por el Procurador Público de la Contraloría General o el Procurador del Sector o el representante legal de la entidad examinada, en los casos en que en la ejecución directa de una acción de control se encuentre daño económico o presunción de ilícito penal. Asimismo, ejerce la potestad para sancionar a los funcionarios o servidores públicos que cometan infracciones contra la administración referidas en el subcapítulo II sobre el proceso para sancionar en materia de responsabilidad administrativa funcional.

- Normar y velar por la adecuada implantación de los Órganos de Auditoría Interna, requiriendo a las entidades el fortalecimiento de dichos órganos con personal calificado e infraestructura moderna necesaria para el cumplimiento de sus fines.

- Presentar anualmente al Congreso de la República el Informe de Evaluación a la Cuenta General de la República, para cuya formulación la Contraloría General dictará las disposiciones pertinentes.

- Absolver consultas, emitir pronunciamientos institucionales e interpretar la normativa del control gubernamental con carácter vinculante, y de ser el caso, orientador. Asimismo establecerá mecanismos de orientación para los sujetos de control respecto a sus derechos, obligaciones, prohibiciones e incompatibilidades previstos en la normativa de control.

- Aprobar el Plan Nacional de Control y los planes anuales de control de las entidades.

- Efectuar las acciones de control ambiental y sobre los recursos naturales, así como sobre los bienes que constituyen el Patrimonio Cultural de la Nación, informando semestralmente sobre el resultado de las mismas y sobre los procesos administrativos y judiciales, si los hubiere, a las comisiones competentes del Congreso de la República.

- Emitir opinión previa vinculante sobre adquisiciones y contrataciones de bienes, servicios u obras, que conforme a ley tengan el carácter de secreto militar o de orden interno exonerados de Licitación Pública, Concurso Público o Adjudicación Directa.

- Otorgar autorización previa a la ejecución y al pago de los presupuestos adicionales de obra pública, y de las mayores prestaciones de supervisión en los casos distintos a los adicionales de obras, cuyos montos excedan a los previstos en la Ley de Contrataciones y Adquisiciones del Estado, y su Reglamento respectivamente, cualquiera sea la fuente de financiamiento.

- Informar previamente sobre las operaciones, fianzas, avales y otras garantías que otorgue el Estado, inclusive los proyectos de contrato, que en cualquier forma

comprometa su crédito o capacidad financiera, sea que se trate de negociaciones en el país o en el exterior.

- Designar de manera exclusiva, Sociedades de Auditoría que se requieran, a través de Concurso Público de Méritos, para efectuar Auditorías en las entidades, supervisando sus labores con arreglo a las disposiciones de designación de Sociedades de Auditoría que para el efecto se emitan.

- Requerir el apoyo y/o destaque de funcionarios y servidores de las entidades para la ejecución de actividades de control gubernamental.

- Recibir y atender denuncias y sugerencias de la ciudadanía relacionadas con las funciones de la administración pública, otorgándoles el trámite correspondiente sea en el ámbito interno, o derivándolas ante la autoridad competente; estando la identidad de los denunciantes y el contenido de la denuncia protegidos por el principio de reserva.

- Promover la participación ciudadana, mediante audiencias y/o sistemas de vigilancia en las entidades, con el fin de coadyuvar en el control gubernamental.

- Participar directamente y/o en coordinación con las entidades en los procesos judiciales, administrativos, arbitrales u otros, para la adecuada defensa de los intereses del Estado, cuando tales procesos incidan sobre recursos y bienes de éste.

- Recibir, registrar, examinar y fiscalizar las Declaraciones Juradas de Ingresos y de Bienes y Rentas que deben presentar los funcionarios y servidores públicos obligados de acuerdo a Ley.

- Verificar y supervisar el cumplimiento de las disposiciones sobre prohibiciones e incompatibilidades de funcionarios y servidores públicos y otros, así como de las referidas a la prohibición de ejercer la facultad de nombramiento de personal en el Sector Público en casos de nepotismo, sin perjuicio de las funciones conferidas a los órganos de control.

- Citar y tomar declaraciones a cualquier persona cuyo testimonio pueda resultar útil para el esclarecimiento de los hechos materia de verificación durante una acción de control, bajo los apremios legales señalados para los testigos.

- Dictar las disposiciones necesarias para articular los procesos de control con los Planes y Programas Nacionales, a efecto de visualizar de forma integral su cumplimiento, generando la información pertinente para emitir recomendaciones generales a los Poderes Ejecutivo y Legislativo sobre la administración de los recursos del Estado, en función a las metas previstas y las alcanzadas, así como brindar asistencia técnica al Congreso de la República, en asuntos vinculados a su competencia funcional.

- Emitir disposiciones y/o procedimientos para implementar operativamente medidas y acciones contra la corrupción administrativa, a través del control gubernamental, promoviendo una cultura de honestidad y probidad de la gestión pública, así como la adopción de mecanismos de transparencia e integridad al interior de las entidades, considerándose el concurso de la ciudadanía y organizaciones de la sociedad civil.

- Establecer los procedimientos para que los titulares de las entidades rindan cuenta oportuna ante el Órgano Rector, por los fondos o bienes del Estado a su cargo, así como de los resultados de su gestión.

- Asumir la defensa del personal de la Institución a cargo de las labores de control, cuando se encuentre incurso en acciones legales, derivadas del debido cumplimiento de la labor funcional, aun cuando al momento de iniciarse la acción, el vínculo laboral con el personal haya terminado.

- Establecer el procedimiento selectivo de control sobre las entidades beneficiarias por las mercancías donadas provenientes del extranjero.

- Ejercer el control de desempeño de la ejecución presupuestal, formulando recomendaciones que promuevan reformas sobre los sistemas administrativos de las entidades sujetas al Sistema.

- Regular el procedimiento, requisitos, plazos y excepciones para el ejercicio del control previo externo, así como otros encargos que se confiera al organismo Contralor, emitiendo la normativa pertinente que contemple los principios que rigen el control gubernamental.

- Celebrar Convenios de cooperación interinstitucional con entidades o privadas, nacionales o extranjeras.

Las citadas atribuciones no son taxativas, comprendiendo las demás que señale la citada Ley y otros dispositivos legales.

La Contraloría General goza de autonomía económica, administrativa, financiera y funcional, conforme a la Constitución Política del Perú y su Ley Orgánica Ley N° 27785 y sus

modificatorias. Para garantizar el cumplimiento de sus objetivos institucionales, la Contraloría General se encuentra exonerada de la aplicación de las normas que establezcan restricciones y/o prohibiciones a la ejecución presupuestaria.

La Contraloría General tiene su sede central en Jesús María, Lima, Perú, y para su desempeño desconcentrado cuenta con 4 Gerencias de Coordinación Regional Lima Metropolitana, Lima Provincias, Centro (Huancayo), Norte (Chiclayo) y Sur (Arequipa), de quien dependen las 27 Contralorías Regionales en las ciudades de Abancay, Arequipa, Ayacucho, Cajamarca, Callao, Chachapoyas, Chiclayo, Chimbote, Cusco, Huancavelica, Huánuco, Huancayo, Huaraz, Ica, Iquitos, Lima Metropolitana, Lima Provincias, Moquegua, Moyobamba, Piura, Pucallpa, Puerto Maldonado, Puno, Tacna, Trujillo y Tumbes, como órganos desconcentrados en el ámbito nacional, con el objeto de optimizar la labor de control gubernamental.

Dichos órganos desconcentrados tienen como finalidad planear, organizar, dirigir, ejecutar y evaluar las acciones de control en las entidades descentralizadas bajo su ámbito.

Conforme lo dispuesto en la Ley N° 27785 y modificatorias - Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, la Contraloría General tiene la facultad de aplicar directamente sanciones por la comisión de las infracciones que hubieren cometido las entidades sujetas a control, sus funcionarios y servidores públicos, las sociedades de auditoría y las personas jurídicas y naturales que manejen recursos y bienes del Estado, o a quienes haya requerido información o su presencia con relación a su vinculación jurídica con las entidades.

2.2.6. Sistema Nacional de Control

En el Perú, el Sistema Nacional de Control, fue creado por Decreto Ley N° 19039 – Ley Orgánica del SNC, de 16.NOV.71, el cual definió y reguló su ámbito, organización,

obligaciones, responsabilidades y sanciones. Su Reglamento, fue aprobado por D.S. Nº 001-72-CG de 7 de marzo de 1972. Posteriormente, el Art. 146º de la Constitución Política de 1979, precisó: "La Ley establece la organización, atribuciones y responsabilidades del SNC" •El Art. 82º de la Constitución de 1993, señala que la Contraloría General es el órgano superior del Sistema Nacional de Control. •En la actual Ley 27785, de 22.JUL.2002, el Título II – Sistema Nacional de Control, se establece: Capítulo I - Concepto y conformación del Sistema (Arts. 12º al 14º)

En el Perú, el sistema de control gubernamental se aplica sobre el funcionamiento de los sistemas administrativos de los recursos públicos y sobre los sistemas funcionales; comprendiendo las estructuras de Control Interno del sector público; así como, por el régimen de responsabilidad que estipula y está previsto en el marco legal y normativo de los funcionarios y servidores públicos. •En algunos países, debido a la imposibilidad física del organismo contralor para ejercer por sí solo, integralmente, el control gubernamental sobre un complejo universo de entidades y órganos que integran la administración pública, y la coexistencia de los órganos de control externo e interno que actúan aisladamente, sin coordinación entre si y sin unidad de planes, objetivos y metas; se ha implementado un Sistema Nacional de Control, como es el caso del Perú.

2.2.7. Ley N° 27785 - Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República

En su segundo artículo señala que, "Es objeto de la ley propender al apropiado, oportuno y efectivo ejercicio del control gubernamental, para prevenir y verificar, mediante aplicación de principios, sistemas y procedimientos técnicos, la correcta, eficiente y transparente utilización y gestión de los recursos y bienes del Estado, el desarrollo honesto y probo de las funciones y actos de las autoridades, funcionarios y servidores públicos, así como

el cumplimiento de metas y resultados obtenidos por las instituciones sujetas a control, con la finalidad de contribuir y orientar al mejoramiento de sus actividades y servicios en beneficio de la Nación".

El capítulo II precisa que el control gubernamental es interno y externo; a su vez el control interno es previo, simultáneo y posterior.

El control interno previo y simultáneo, compete exclusivamente a las autoridades, funcionarios y servidores públicos de las entidades como responsabilidad propia de las funciones que le son inherentes, sobre la base de las normas que rigen las actividades de la organización y los procedimientos establecidos en sus planes, reglamentos, manuales y disposiciones institucionales, los que contienen las políticas y. métodos de autorización, registro, verificación, evaluación, seguridad y protección.

El control interno es un proceso continuo realizado por la dirección, la gerencia y, el personal de la entidad; para proporcionar seguridad razonable, respecto a si está lográndose los objetivos siguientes:

- Promover la efectividad, eficiencia y economía en las operaciones y, la calidad en los servicios que debe brindar cada entidad pública;
- Proteger y conservar los recursos públicos contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal;
- Cumplir las leyes, reglamentos y otras normas gubernamentales; y,
- Elaborar información financiera válida y confiable, presentada con oportunidad.

El Control Interno está dirigido a coadyuvar con la administración pública al logro de sus objetivos institucionales; es parte inherente a las actividades de control previo y concurrente (De responsabilidad de las autoridades, funcionarios y servidores públicos), lo cual

lo hace complementario al Control Gubernamental explicado líneas arriba y normado por la Ley N° 27785.

Para que el control interno cumpla con sus objetivos debe considerarse en su implantación los cinco (5) componentes, los que se integran en el proceso de gestión y operan en distintos niveles de efectividad y eficiencia.

Para operar la estructura de control interno se requiere la implementación de sus componentes (Ambiente de Control Interno, Evaluación del Riesgo, Actividades de Control Gerencia Sistema de Información y Comunicaciones, Actividades Monitoreo), los mismos que se encuentran interrelacionados e integrados al proceso administrativo. Los componentes pueden considerarse como un conjunto de normas que son utilizadas para medir el control interno y determinar su efectividad, los que se describen a continuación:

a. ***Ambiente de Control Interno***. *Se refiere al establecimiento de un entorno que estimule e influencie las tareas de las personas con respecto al control de sus actividades. Como el personal resulta ser la esencia de cualquier entidad, sus atributos constituyen el motor que según el Artículo 6° de la Ley N"27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, conduce y la base sobre la que todo descansa. Son elementos del ambiente de control, entre otros, integridad y valores éticos, estructura orgánica, asignación de autoridad y responsabilidad y políticas para la administración de personal.*

b. ***Evaluación del Riesgo.*** *El riesgo se define como la probabilidad de que un evento o acción afecte adversa mente a la entidad. Su evaluación implica la identificación, análisis y manejo de los riesgos relacionados con la elaboración de estados financieros y que pueden incidir en el logro de los objetivos del control interno en*

la entidad. Estos riesgos incluyen eventos o circunstancias internas o externas que pueden afectar el registro, procesamiento y reporte de información financiera, así como las representaciones de la gerencia en los estados financieros. Son elementos de la evaluación del riesgo, entre otros, cambios en el ambiente operativo del trabajo, ingreso de nuevo personal, implementación de sistemas de información nuevos y reorganización en la entidad. La evaluación de riesgos debe ser responsabilidad de todos los niveles gerenciales involucrados en el logro de objetivos. Esta actividad de auto-evaluación que práctica la dirección debe ser revisada por los auditores para asegurar que los objetivos, enfoque, alcance y procedimientos han sido apropiadamente realizados.

c. ***Actividades de Control Gerencial****. Se refieren a las acciones que realizan la gerencia y otro personal de la entidad para cumplir diariamente con las funciones asignadas. Son importantes porque en sí mismas implican la forma correcta de hacer las cosas, así como también porque el dictado de políticas y procedimientos y la evaluación de su cumplimiento, constituyen medios idóneos para asegurar el logro de objetivos de la entidad. Son elementos de las actividades de control gerencial, entre otros, las revisiones del desempeño, el procesamiento de información computarizada, los controles relativos a la protección y conservación de los activos, así como la división de funciones y responsabilidades.*

d. ***Sistema de Información y Comunicación.*** *Está constituido por los métodos y procedimientos establecidos para registrar, procesar, resumir e informar sobre las operaciones financieras de una entidad. La calidad de la información que brinda el sistema afecta la capacidad de la gerencia para adoptar decisiones adecuadas que permitan controlar las actividades de la entidad. En el sector público el sistema integrado de información financiera debe propender al uso de una base de datos*

central y única, soportada por tecnología informática y telecomunicaciones, accesible para todos los usuarios de las áreas de presupuesto, tesorería, endeudamiento público y contabilidad gubernamental, en el nivel central y en el nivel operativo y, para los administradores gubernamentales. La comunicación implica proporcionar un apropiado entendimiento sobre los roles y responsabilidades individuales involucradas en el Control Interno de la información financiera dentro de una entidad.

e. ***Actividades de Monitoreo o Seguimiento***. *Representan al proceso que evalúa la calidad del control interno en el tiempo y permite al sistema reaccionar en forma dinámica, cambiando cuando las circunstancias así lo requieran. Se orienta a la identificación de controles débiles, insuficientes o innecesarios y, promueve su reforzamiento. El monitoreo se lleva a cabo de tres formas: (a) durante la realización de actividades diarias en los distintos niveles de la entidad; (b) de manera separada por personal que no es el responsable directo de la ejecución de las actividades, incluidas las de control; y, (c) mediante la combinación de ambas modalidades.*

El enfoque de Ley tiende a convertir el control interno en una de las herramientas de la administración pública que coadyuve a lograr objetivos institucionales con eficiencia, eficacia, oportunidad, transparencia y economía, toda vez que las estadísticas de la Contraloría General indican que la mayor causa de las deficiencias e irregularidades detectadas en la administración pública es la presión que ejercen los niveles superiores jerárquicos sobre los niveles intermedios o inferiores, induciéndolos a la transgresión de sus normas internas institucionales como: el ROF, MOF, Manual de Procedimientos, los mismos que fueron aprobados por el titular de la institución y que dicho sea de paso, no son coercitivos ni generan una sanción ejemplar en caso de incumplimiento.

2.2.8. Control Interno

Control Interno: Su definición de acuerdo a los modelos contemporáneos de Control Interno. La concepción de control interno ha sufrido modificaciones en la medida en que se han transformado las estructuras organizacionales, para ello toma como base la manera en que ha evolucionado la auditoria, Mantilla y Blanco (2005, pp. 26-29) evidencian tres generaciones de control interno: "Primera generación: esta etapa de control interno se basó en acciones empíricas a partir de procedimientos de ensayo y error" (Revista venezolana, 2011). Esta generación, si bien es obsoleta aún tiene una fuerte aplicación generalizada. La principal causa de su insistente aplicación se debe en buen aparte a la carente profesionalización de quienes tienen a su cargo el sistema de control interno. Dicha etapa estuvo fuertemente relacionada con los controles contables y administrativos; Segunda generación: Esta etapa se encuentra marcada por el sesgo legal. Se logran imponer estructuras y prácticas de control interno, especialmente en el sector público, pero desafortunadamente dio una conciencia distorsionada de este, al hacerlo operar muy cerca de la línea de cumplimiento (formal) y lejos de los niveles de calidad (técnicos), se da como centro de atención la evaluación del control interno como el medio para definir el alcance de las pruebas de auditoria, Por ende, el control interno comprende el plan de organización y el conjunto de métodos y procedimientos que aseguren que los activos están debidamente protegidos, que los registros contables son fidedignos y que las actividades de la entidad se desarrollan eficazmente según las directrices señaladas por la administración; Tercera generación: Actualmente centra esfuerzos en la calidad derivada del posicionamiento en los más altos niveles estratégicos y directivos, como requisito que garantiza la eficiencia del control interno.

Es aquí donde se reconoce el fruto de los esfuerzos originados por COSO hacia los años 90's, los cuales han sido complementados por los nuevos direccionamientos estratégicos, el

ascenso en la escala organizacional y, reforzados por los alcances de la Sarbanes-Oxley Acta de 2002.

"En la última década los controles internos han tomado una orientación dirigida de manera prioritaria a fomentar la eficiencia, reduciendo el riesgo en la consecución de los objetivos, ayudan a asegurar la confiabilidad de la información financiera y la de gestión, a proteger los recursos, y a cumplir las leyes, reglamentos y cláusulas contractuales aplicables. Coopers y Lybrand (1997, p. 04), Define al control interno desde el punto de vista del modelo COSO así: "Es un proceso ejecutado por el consejo de directores, la administración y el resto del personal de una entidad, diseñado para proporcionar seguridad razonable con miras a la consecución de objetivos en las siguientes categorías: - Efectividad y eficiencia de las operaciones; - Confiabilidad en la información financiera; - Cumplimiento de las leyes y regulaciones aplicables. "Con base a esta definición entonces, el control interno es una serie de acciones concatenadas y realizadas por todos los miembros de la entidad, orientados a la consecución de las metas organizacionales, a prevenir la pérdida de recursos, a asegurar información financiera confiable y que la empresa cumpla con las leyes y regulaciones aplicables. Resalta la idea de que el control interno efectivo solo puede ayudar a la organización a lograr sus objetivos más no asegura el éxito organizacional". Por otra parte, se tiene la definición de control interno mostrada en el modelo COCO (Criteria of Control) de Canadá, fue publicado tres años más tarde que COSO; éste simplifica los conceptos y el lenguaje para hacer posible una discusión sobre el alcance total del control, con la misma facilidad en cualquier nivel de la organización empleando un lenguaje accesible para todos los empleados. Estupiñán, (2006: 09) al respecto expone, "El modelo COCO es producto de una profunda revisión del comité de criterios de control de Canadá sobre el reporte COSO y cuyo propósito que hacer el planteamiento de un modelo más sencillo y comprensible, ante las dificultades que en la aplicación del COSO enfrentaron inicialmente algunas organizaciones. El

resultado es un modelo conciso y dinámica encaminado a mejorar el control, el cual describe y define al control casi de forma idéntico a como lo hace el modelo COSO". (Rivas, 2014).

Lazcano, citado por Quevedo y Ramírez (2006: 47) define el control interno desde el punto de vista de este modelo así: "El control incluye aquellos elementos de una organización (recursos, sistemas, procesos, cultura, estructura y metas) que tomadas en conjunto apoyan al personal en el logro de los objetivos de la entidad. Estos objetivos pueden referirse a una o más de las siguientes categorías: - Efectividad y eficiencia de las operaciones; - Confiabilidad de los reportes internos o para el exterior; - Cumplimiento con las leyes y reglamentos aplicables así como con las políticas internas".

Por otro lado, la concepción del control interno, se encuentra la definición mostrada en el llamado modelo MICIL que surge como una respuesta a la necesidad de establecer un enfoque apropiado a la realidad de Latinoamérica, por esto el Marco Integrado de Control Interno para Latinoamérica procura establecer un marco de referencia para las necesidades y las expectativas de los directores de las empresas privadas de las instituciones públicas, de las organizaciones de la sociedad civil y de otros interesados, este modelo define al control interno así MICIL (2004: 01): "El control interno es un proceso aplicado en la ejecución de las operaciones, ejecutado por los funcionarios y servidores que laboran en las organizaciones, debe aportar un grado de seguridad razonable y debe orientarse a facilitar la consecución de los objetivos institucionales: eficiencia y eficacia de las operaciones, confiabilidad de la información financiera y operativa, protección de los activos, cumplimiento de las leyes, regulaciones y contratos.

2.2.9. Fases para el proceso de implementación del Sistema Control Interno:

a. Planificación, la cual tiene como objetivo la formulación de un Plan de Trabajo que incluya los procedimientos orientados a implementar adecuadamente el SCI, en

base a un diagnóstico previamente elaborado. Son aspectos inherentes a esta fase asegurar el compromiso de la Alta Dirección y la conformación de un comité de Control Interno.

b. Ejecución, en la que se implantará el SCI en sus procesos, actividades, recursos, operaciones y actos institucionales, para lo cual la entidad procede al desarrollo del Plan de Trabajo para la implantación del SC!.

c. Evaluación, en la que se evalúan los avances logrados y las limitaciones encontradas en el proceso de implementación como parte de la autoevaluación mencionada en el componente de Supervisión.

2.2.10. Naturaleza del Sistema de Control Interno y su implementación en el sector público.

El Control Gubernamental consiste en la supervisión, vigilancia y verificación de los actos y resultados de la gestión pública, en atención al grado de eficiencia, eficacia, transparencia y economía en el uso y destino de los recursos y bienes del Estado, así como del cumplimiento de las normas legales y de los lineamientos de política y planes de acción, evaluando los sistemas de administración, gerencia y control, con fines de su mejoramiento a través de la adopción de acciones preventivas y correctivas.

El control gubernamental es interno y externo y su desarrollo constituye un proceso integral y permanente.

El Control Interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúen correcta y eficientemente.

Es responsabilidad del Titular de la entidad fomentar y supervisar el funcionamiento y confiabilidad del control interno para la evaluación de la gestión y el efectivo ejercicio de la

rendición de cuentas, propendiendo a que éste contribuya con el logro de la misión y objetivos de la entidad a su cargo.

El Sistema de Control Interno, se define al conjunto de acciones, actividades, planes, políticas, normas, registros, organización, procedimientos y métodos, incluyendo la actitud de las autoridades y el personal, organizados e instituidos en cada entidad del Estado, para la consecución de los objetivos siguientes:

a. Promover y optimizar la eficiencia, eficacia, transparencia y economía en las operaciones de la entidad, así como la calidad de los servicios públicos que presta.

b. Cuidar y resguardar los recursos y bienes del Estado contra cualquier forma de pérdida, deterioro, uso indebido y actos ilegales, así como, en general, contra todo hecho irregular o situación perjudicial que pudiera afectarlos.

c. Cumplir la normatividad aplicable a la entidad y a sus operaciones.

d. Garantizar la confiabilidad y oportunidad de la información.

e. Fomentar e impulsar la práctica de valores institucionales.

f. Promover el cumplimiento de los funcionarios o servidores públicos de rendir cuentas por los fondos y bienes públicos a su cargo o por una misión u objetivo encargado y aceptado.

Cabe indicar, que las entidades del estado implantan obligatoriamente sistemas de control interno en sus procesos, actividades, recursos, operaciones y actos institucionales, orientando su ejecución al cumplimiento de los objetivos mencionados en el párrafo anterior.

La Resolución de Contraloría Nº 320-2006-CG, que aprueba las Normas de Control Interno, señala, entre otros:

- Que son principios aplicables al SCI: (i) el autocontrol, (ii) la autorregulación, y (iii) la autogestión.

- Que el enfoque moderno establecido por el COSO, la Guía de INTOSAI y la Ley Nº 28716, señala que los componentes de la estructura de control interno se interrelacionan entre sí y comprenden diversos elementos que se integran en el proceso de gestión. Por ello, para fines de la adecuada formalización e implementación de la estructura de control interno en todas las entidades del Estado, se concibe que ésta se organice con base a cinco (5) componentes:
    a. *Ambiente de control*
    b. *Evaluación de riesgos*
    c. *Actividades de control gerencial*
    d. *Información y comunicación*
    e. *Supervisión.*

Posteriormente, con la Resolución de Contraloría Nº 458-2008-CG de 30 de octubre de 2008, se aprobó la "Guía para la Implementación del SCI de las entidades del Estado", cuyo objetivo principal es la de proveer de lineamientos, herramientas y métodos a las entidades del Estado para la implementación de los componentes que conforman el SCI establecido en las Normas de Control Interno Además, permitirá realizar una adecuada implementación del SCI en la gestión de las operaciones de la entidad, con la finalidad de fortalecer la organización y contribuir al logro de sus objetivos, siempre de acuerdo con la naturaleza de sus actividades.

El Decreto de Urgencia Nº 067-2009 emitido el 23 de junio de 2009, dispone *"modificar el Art. 10º de la Ley Nº 28716"*, incorporando como cuarto párrafo del artículo en mención, lo siguiente:

"*El marco normativo y la normatividad técnica de control que dicte la Contraloría General de la República a que se refiere el párrafo anterior serán de aplicación progresiva, teniendo en cuenta la naturaleza de las funciones de las entidades, así como la disponibilidad de*

recursos presupuestarios, debiendo entrar en vigencia cuando se culmine la aprobación de todas las Leyes de Organización y Funciones de los diversos Sectores de Gobierno Nacional y de sus respectivos documentos de gestión, así como cuando el SIAF SP versión II, el cual incluirá el módulo de evaluación de Control Interno, esté implementado en los tres niveles de gobierno".

Consecuentemente quedaban sin efecto los plazos establecidos, más no la obligación de adecuar el SCI, a las disposiciones dictadas.

Posteriormente, se emite la Ley Nº 29743 de 9 de julio de 2011, que aprueba "*modificar el Art. 10º de la Ley Nº 28716*", en la que señala sustitúyase el cuarto párrafo del artículo en mención, por el siguiente texto:

"El marco normativo y la normativa técnica de control que emite la Contraloría General de la República en el proceso de implantación del SCI, toma en cuenta la naturaleza de las funciones de las entidades, proyectos de inversión, actividades y programas sociales que estas administran".

Muy independientemente a lo señalado en estos dos últimos dispositivos (Decreto de Urgencia Nº 067-2009 y la Ley Nº 29743), está vigente lo señalado en el cuarto párrafo de la Ley Nº 27785, tercer párrafo del Artículo 4º de la Ley Nº 28716, y el Artículo 6º de la Ley Nº 28716. Tener en cuenta lo señalado en el Artículo 8º de la Ley Nº 28716 que señala textualmente lo siguiente:

"La inobservancia de la presente Ley, genera responsabilidad administrativa funcional, y da lugar a la imposición de la sanción de acuerdo a la normativa aplicable, sin perjuicio de la responsabilidad civil o penal a que hubiere lugar, de ser el caso".

2.2.11. Organización y funciones de las oficinas de Tecnologías de la Información

Dependiendo de la complejidad de las mismas; para efectos de este estudio las hemos clasificado en oficinas de alta, mediana y pequeña complejidad.

A continuación, se describe las actividades y funciones de estas oficinas teniendo en cuenta su estructura orgánica, adquisiciones de hardware y software, mantenimiento de los mismos y gestión de la seguridad informática, las cantidades que se presentan en los cuadros estadísticos se refieren solo a adquisiciones o servicios de mantenimiento que por su materialidad son objeto de auditoría.

A. Oficinas de alta complejidad. En ella se encuentran las superintendencias, reguladoras, ministerios, empresas eléctricas, organismos autónomos, servicios de administración tributaria, entre otras.

Estructura orgánica:.- Estas oficinas cuentan con Reglamento de Organización y Funciones, Manual de Organización y Funciones, Plan Estratégico de Tecnologías de Información y Plan Operativo Informático, donde se detalla la visión, misión objetivos y estrategias; así como las funciones y atribuciones inherentes a cada cargo.

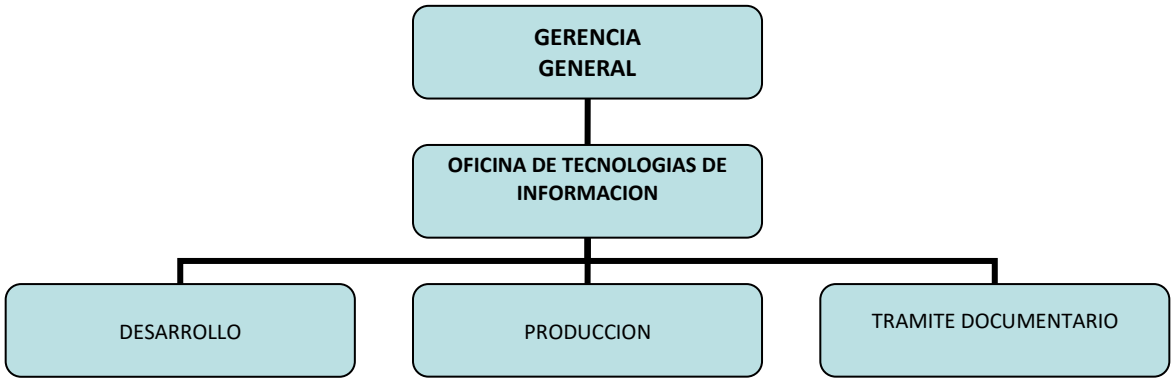
El Plan Operativo informático es elaborado siguiendo los lineamientos de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI de la Presidencia del Consejo de Ministros – PCM y sirve como un instrumento para el seguimiento, supervisión y evaluación de las actividades programadas.

A continuación presentamos dos organigramas típicos de este tipo de oficinas (véase figura 04 y 05); en la cual se puede observar que tienen claramente definidas las áreas de desarrollo, encargada del: análisis y diseño de sistemas y producción, soporte técnico al hardware y software instalado en la entidad. En promedio, el número de trabajadores de estas oficinas de TIC´s es mayor a quince. Jerárquicamente, la mayoría de estas oficinas son órganos

de línea que dependen de la Dirección General o Gerencia General; tienen asignado un presupuesto anual; en base a objetivos previamente establecidos; pero la ejecución del gasto lo realiza la oficina de administración.

Figura 1

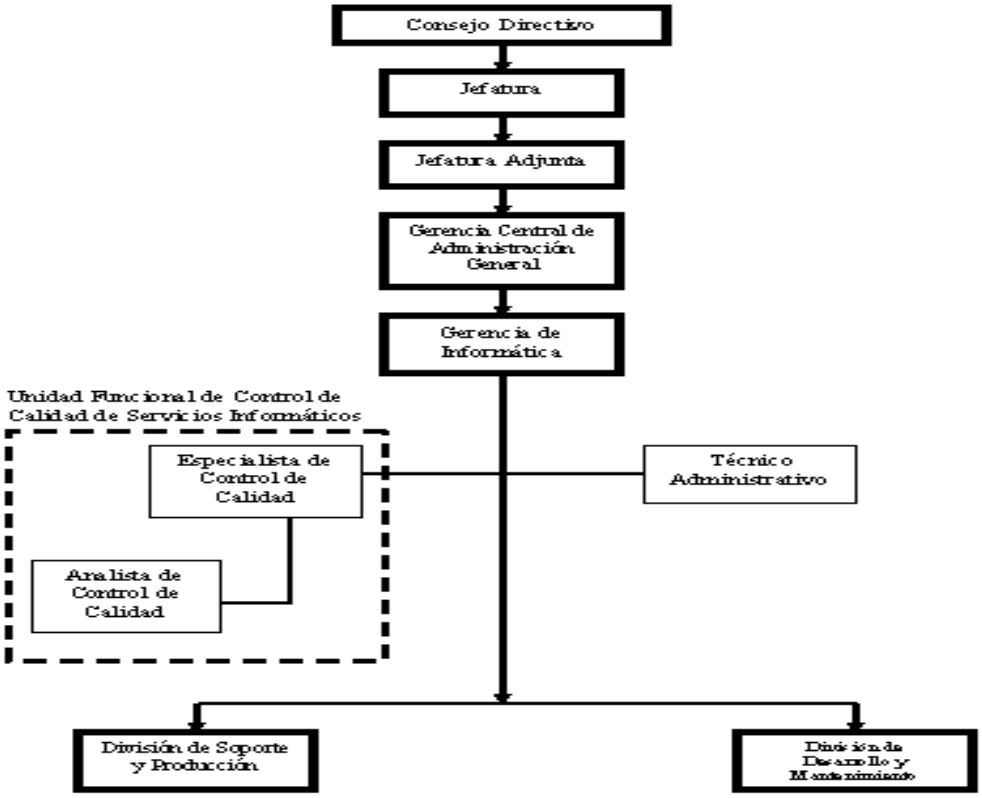
Organigrama del área TI



Nota. Elaborado en base al Reglamento de Organización y Funciones y Plan Operativo Informático 2017 de la OSCE.

Figura 2

Organigrama general del área de una unidad de TI



Nota. Elaborado en base al Manual de Organización y Funciones y Plan Operativo Informático 2018 del SAT de la Municipalidad metropolitana de Lima

Adquisiciones de hardware y software.- Las compras obedecen a un plan anual debidamente aprobado por la alta dirección; se orientan básicamente a servidores de red de alta gama, grandes lotes de equipos de cómputo y licencias de software.

Mantenimiento del hardware y software.- El mantenimiento de los equipos de cómputo se realiza en virtud a lo previsto en los planes de mantenimiento preventivo, documento que contempla por separado los cronogramas de mantenimiento preventivo de los servidores, computadoras personales, laptops, impresoras, switches y UPSs; tanto para los equipos con

garantía vigente como para los que se encuentran con garantía vencida. El mantenimiento correctivo también lo realiza el personal de informática; en caso que no encuentre la solución acude a terceros.

El mantenimiento de los sistemas desarrollados en la entidad está a cargo de la Oficina de Desarrollo para lo cual analiza los requerimientos del usuario, diseña y desarrollo la solución y realiza las pruebas necesarias en un equipo configurado para este fin. Las pruebas se realizan en coordinación con el usuario y son puestas a producción una vez que el control de calidad es satisfactorio.

El soporte técnico a los sistemas desarrollados por el Ministerio de Economía y Finanzas (SIGA, SIAF, SISPER) es brindado por el personal de soporte técnico en coordinación con sectoristas del MEF, quienes también se hacen presente a solicitud de los usuarios. El control de accesos al SIGA, SIAF y demás sistemas es administrado por la Jefatura de Informática.

Seguridad de la información**.-** El manejo de la información se reglamenta en lineamientos de política y directivas relacionadas con la seguridad de la Información, en aplicación de las normas técnicas adoptadas por el estado, orientadas a preservar la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos que identifica riesgos y adopta los controles y procedimientos eficaces para salvaguardar la información de la organización; sin embargo, a pesar de que el uso obligatorio, en todas las entidades integrantes del Sistema Nacional de Informática, de la Norma Técnica Peruana "NTP-ISO/IEC17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas Para la Gestión de la Seguridad de la Información. 2ª Edición", fue aprobado por Resolución Ministerial N° 246-2007-PCM del 22 de agosto de 2007, aun no se ha concretado su implementación en muchas entidades del sector público

Los trabajadores de la Oficina de TIC´s están capacitados en temas de seguridad de la información y mantienen un control permanente sobre la implementación de las políticas y normas especificadas.

El Plan de Contingencias Informático es elaborado por consultoría externa y está dividido en dos grupos:

- Plan de Contingencias de los Sistemas de Información, que incluye: Plan de Riesgos, Plan de Recuperación de Desastres, Políticas de Seguridad
- Plan de Contingencias de la Red, que comprende: análisis de riesgos, principales método de protección, técnicas y tecnologías de seguridad a nivel de red, seguridad en redes, seguridad en redes Linux, procedimientos para la recuperación de desastres.

Estos planes pretenden analizar dos ámbitos: El primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarlas. El segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está operativo y actualizado

Para resguardar la seguridad física de la información pocas entidades, como la OSCE y el SAT de la Lima, han instalado dos centros de cómputo que cuentan con modernos sistemas perimetrales de seguridad, energía permanente y estabilizada y están interconectados mediante un enlace dedicado de fibra óptica de extremo a extremo de tipo permanente o dedicado, que permite contar con un esquema de transmisión de datos (cluster de servidores y replicación de base de datos entre sistemas de almacenamiento) entre las dos salas de servidores.

El procedimiento de generación de copias de respaldo se realiza automáticamente mediante el uso de un servidor de almacenamiento (Hp storage Works), este esquema se replica

en las dos salas de servidores de la entidad; las copias son retiradas por personal de la Oficina de TIC y remitidas al exterior para su resguardo final.

B. Oficinas de mediana complejidad. La conforman los gobiernos regionales, universidades, municipalidades de las capitales de región, empresas municipales de agua potable, proyectos especiales, etc.

Estructura orgánica.- La mayoría solo cuenta con Reglamento de Organización y Funciones, Manual de Organización y Funciones y Plan Operativo Informático, donde se detalla la visión, misión y objetivos; así como las funciones y atribuciones inherentes a cada cargo.

El Plan Operativo informático es elaborado solo para cumplir con las formalidades exigidas mediante ley por la ONGEI de la PCM y muy pocos lo utilizan como una herramienta para la gestión. En promedio, el número de trabajadores de estas oficinas de TIC´s está entre cuatro y catorce.

Orgánicamente el área de Informática de este tipo de entidades es un órgano de apoyo a la Gerencia Regional o Municipal, está conformado por un Jefe, un equipo encargado del soporte técnico y otro encargado del mantenimiento de los sistemas o del portal web

Adquisiciones de hardware y software.- Algunas compras obedecen a un plan anual debidamente aprobado por la alta dirección; se orientan básicamente a servidores de red de gama media, lotes medianos de equipos de cómputo solo con licencia de sistema operativo.

Mantenimiento del hardware y software.- Algunas entidades elaboran y dan cumplimiento a su plan de mantenimiento preventivo y otras elaboran solo un cronograma para el mantenimiento de los equipos de cómputo. Estos planes no son evaluados y no existen bitácoras o fichas de mantenimiento que evidencien la ejecución del plan. Tampoco existe evidencia del mantenimiento realizado por los proveedores durante el periodo de garantía.

El mantenimiento correctivo también lo realiza el personal de soporte técnico; en caso que no encuentren la solución acude a terceros.

El software implementado en estas entidades, es el desarrollado por el Ministerio de Economía y Finanzas (SIGA, SIAF, SISPER) y su mantenimiento es brindado por el personal del equipo de Desarrollo en coordinación con sectoristas del MEF, quienes también se hacen presente a solicitud de los usuarios. El control de accesos al SIGA, SIAF y demás sistemas es administrado por la Jefatura de Informática.

Seguridad de la información.- Elaboraron el plan de contingencias para cumplir con la normativa, pero no lo aplican; además no poseen normas internas que orienten la gestión del servicio informático, debidamente aprobados como son:

- Políticas de seguridad,
- Manuales de los sistemas,
- Planes de mantenimiento, de contingencia, etc.
- Procedimientos para control de las cuentas de los usuarios, mantenimiento de hardware y software, uso del internet y correo electrónico, uso de dispositivos móviles en lugares públicos, respaldo de la información, gestión de pistas de auditoría, entre otros.

En cuanto a la seguridad física, se observa lo siguiente:

- El cableado de red se encuentra muy expuesto, en muchos casos está al aire libre y las canaletas están mal instaladas.
- Existen diversas marcas de equipos de comunicaciones, lo cual no permite estandarizar configuraciones y optimizar el desempeño de la red de datos.

- Los cables y puntos de red no están rotulados, lo cual hace más difícil la administración del cableado de datos, generando mayores tiempos de respuesta ante la falla de algún punto de red.
- En muchos casos los equipos de comunicaciones no están dispuestos en racks protegidos con llave; exponiendo los equipos a cualquier amenaza interna o externa de manipulación o sabotaje.
- Algunos switches de comunicaciones no están protegidos por sistemas de alimentación ininterrumpida - UPS´s y en muchos casos la puesta a tierra carece de mantenimiento.
- Las copias de respaldo no se ejecutan dentro de los plazos previstos y se realizan copias solo en el disco duro de otra computadora.

C. Oficinas de poca complejidad. En este grupo se encuentran algunas municipalidades provinciales y las distritales, empresas de estas municipalidades y otras entidades públicas con pocos usuarios por atender.

En este grupo se encuentran algunas municipalidades provinciales y las distritales, empresas de estas municipalidades y otras entidades públicas con pocos usuarios por atender. Sus funciones están determinadas el ROF o MOF de la entidad y elaboran el Plan Operativo Informático solo por cumplir con lo establecido por ley. En estas oficinas labora de uno a tres trabajadores y sus estados financieros reportan gastos reducidos en la adquisición de equipos y programas informáticos que por su materialidad no amerita revisión durante una acción de control.

Estas oficinas dependen de la Oficina de Planificación y Presupuesto o de la Oficina General de Administración y, en su mayoría están constituidas por un responsable que tiene a su mando empleados avocados al mantenimiento del hardware.

La creciente demanda del servicio informático ha generado que se requiera de personal adicional cuyas funciones, atribuciones y responsabilidades no están claramente definidas, lo cual dificulta la coordinación, genera duplicidad de esfuerzos, y ha ocasionado que se descuide aspectos tan importantes como:

- La elaboración y evaluación de planes informáticos de corto, mediano y largo plazo, tales como el Plan Operativo Informático y el Plan de Contingencias.

- La asignación de responsabilidades para la ejecución, supervisión y control de los proyectos y actividades considerados en los planes operativos informáticos.

- La definición y aprobación de políticas, procedimientos, estándares y metodologías para el análisis, desarrollo e implementación de sistemas informáticos.

2.3. Marco tecnológico

2.3.1. COSO III

En mayo de 2013 el Comité COSO publicó la actualización del Marco Integrado de Control Interno (COSO I y COSO II) y publicó COSO III, cuyos objetivos son: aclarar los requerimientos del control interno; actualizar el contexto de la aplicación del control interno a muchos cambios en las empresas y ambientes operativos; y ampliar su aplicación; al expandir los objetivos operativos y de emisión de informes. Este nuevo Marco Integrado permite una mayor cobertura de los riesgos a los que se enfrentan actualmente las organizaciones.

El Marco Integrado de Control Interno, definido por COSO III; establece tres categorías de objetivos, cinco componentes y diecisiete principios; tal como se muestra en la figura:

Figura 3

Componentes y principios de control interno

Nota. Modelo de control interno COSO 213

Para determinar que el Sistema de Control Interno es efectivo y reducir a un nivel aceptable el riesgo de no alcanzar un objetivo; los cinco componentes deben funcionar de manera integrada. Los componentes son interdependientes, existe una gran cantidad de interrelaciones y vínculos entre ellos.

Así mismo, dentro de cada componente el marco establece 17 principios que representan los conceptos fundamentales y son aplicables a los objetivos operativos, de información y de cumplimiento. Los principios permiten evaluar la efectividad del sistema de control interno.

La eficacia del sistema de control interno también requiere que los cinco componentes y los principios estén presentes y funcionando:

La implementación del Marco Integrado de Control Interno debe fundamentarse en el modelo de negocios de la entidad, el cual involucra la mayoría de los procesos de administración y gobierno.

El modelo de negocios inicia con el gobierno, el cual incluye la visión y misión de la organización; así como la supervisión del Consejo de Administración de la planificación y las operaciones de la empresa. También incluye las actividades de la Dirección para garantizar la efectividad del establecimiento de la estrategia y demás procesos de gestión de la organización. Un gobierno efectivo asegura la responsabilidad, la rendición de cuentas, la equidad y transparencia en las relaciones de la organización con sus diferentes grupos de interés (accionistas, prestamistas, clientes, proveedores, empleados, gobiernos, reguladores y comunidades en la que opera la organización).

El establecimiento de la estrategia de la organización es el proceso en el que la administración articula un plan de alto nivel para lograr uno o más objetivos en relación con la misión de la organización. Usualmente, la estrategia es presentada en forma de objetivos generales, iniciativas y tácticas. Juntos, estos elementos del gobierno y el establecimiento de la estrategia, proporcionan orientación a la empresa y claramente tienen un lugar para asegurar el éxito de la organización en el cumplimiento de las demandas y expectativas de las partes interesadas.

Dentro del modelo de negocios hay cuatro elementos que se basan en el círculo Deming: planear, hacer, verificar y actuar (plan, do, check, actcycle). En el modelo se presentan como planificación del negocio, ejecución, monitoreo y adaptación.

2.4. Marco legal

Mediante el artículo 6° de la Ley N° 27785, Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, establece que el control gubernamental

consiste en la supervisión, vigilancia y verificación de los actos y resultados de la gestión pública, en atención al grado de eficiencia, eficacia, transparencia y economía en el uso y destino de los recursos y bienes del Estado, así como del cumplimiento de las normas legales y de los lineamientos de política y planes de acción, evaluando los sistemas de administración, gerencia y control, con fines de su mejoramiento a través de la adopción de acciones preventivas y correctivas pertinentes.

El artículo 7° de la citada Ley, establece que el control interno comprende las acciones de cautela previa, simultánea y de verificación posterior que realiza la entidad sujeta a control, con la finalidad que la gestión de sus recursos, bienes y operaciones se efectúe correcta y eficientemente, siendo responsabilidad del Titular de la entidad fomentar y supervisar el funcionamiento y confiabilidad del control interno para la evaluación de la gestión y el efectivo ejercicio de la rendición de cuentas, propendiendo a que éste contribuya con el logro de la misión y objetivos de la entidad a su cargo.

La Ley N° 28716, Ley de Control Interno de las Entidades del Estado, establece que la Contraloría General de la República es la entidad competente para dictar la normativa técnica de control que oriente la efectiva implantación y funcionamiento del control interno en las entidades del Estado, así como su respectiva evaluación.

La Resolución de Contraloría N° 458-2006-CG, que aprobó la "Guía para la Implementación del Sistema de Control Interno de las entidades del Estado" con el objetivo principal de proveer de lineamientos, herramientas y métodos a las entidades del Estado para la implementación de los componentes que conforman el Sistema de Control Interno (SCI) establecido en las Normas de Control Interno (NCI); Que, la Ley N° 30372, Ley del Presupuesto del Sector Público para el Año Fiscal 2016, en su Quincuagésima Tercera Disposición Complementaria Final, establece la obligación de todas las entidades de los tres

niveles de gobierno de implementar su Sistema de Control Interno, en un plazo máximo de treinta y seis (36) meses, contados a partir de su entrada en vigencia; para lo cual la Contraloría General de la República emitirá las disposiciones conteniendo los plazos por cada fase y nivel de gobierno y los demás lineamientos que sean necesarios.

La Directiva N° 013-2016-CG/GPROD denominada "Implementación del Sistema de Control Interno en las Entidades del Estado", aprobada por Resolución de Contraloría N° 149-2016-CG, regula el nuevo modelo y los nuevos plazos para la implementación del Sistema de Control Interno que deben realizar las entidades del Estado en los tres niveles de gobierno; así como la medición del nivel de madurez del SCI con base a la información que deben registrar las entidades de todos los niveles de gobierno en el aplicativo informático Seguimiento y Evaluación del Sistema de Control Interno; Que, en el marco de la citada Directiva y de acuerdo a los cambios del modelo de control interno denominado "Control Interno – Marco Integrado" – COSO, que se utiliza como referencia para la normativa de control interno del país.

La nueva Guía para la implementación y fortalecimiento del Sistema de Control Interno en las entidades del Estado, aprobada mediante la Resolución de contraloría N° 004-2017-CG de 20 de enero de 2017, mediante el cual, se actualiza las orientaciones para las entidades del estado respecto del proceso de implementación del Sistema de Control Interno.

2.5. Marco conceptual

Administración pública.-

Es un sistema de límites imprecisos que comprende el conjunto de organizaciones que realizan la función administrativa y de gestión del Estado[1] y de otros entes públicos con personalidad jurídica, ya sean de ámbito regional o local. Por su función, la Administración Pública pone en contacto directo a la ciudadanía con el poder político,

«satisfaciendo» los intereses públicos de forma inmediata, por contraste con los poderes legislativo y judicial, que lo hacen de forma mediata. (https://es.wikipedia.org/wiki/Administraci%C3%B3n_p%C3%BAblica).

Alerta de control.-

Es el informe en el que se expone de manera concisa y objetiva los indicios de irregularidades identificadas, la norma contravenida, el perjuicio identificado y de ser el caso, y la documentación de sustento correspondiente, lo que se comunica al titular de la entidad con el propósito de que disponga la implementación de medidas correctivas en el marco de las responsabilidades que le competen respecto al ejercicio de control interno. (Directiva N° 011-2015-CG/GPROD de evaluación de denuncias)

Auditoría.-

Examen comprensivo y constructivo de la estructura organizativa de una empresa, institución, departamento gubernamental o de cualquier otra entidad; así como de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales.

Conceptualmente, la auditoría, sea está de cualquier tipo, consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y cumple las condiciones que le han sido prescritas. Con base en lo anterior, podemos descomponer este concepto en los siguientes elementos fundamentales:

- Contenido: una opinión
- Condición: una observación profesional
- Justificación: sustentada en determinados procedimientos
- Objeto: una determinada información obtenida de un soporte
- Finalidad: determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

Comunicación de desviación de cumplimiento.-

La comisión auditora, cautelando el debido proceso comunica de manera escrita y reservada, las desviaciones de cumplimiento debidamente sustentadas, a través de cédulas a las personas que participaron en dichas desviaciones, estén o no prestando servicios en la entidad auditada, en el domicilio real, legal o en el último domicilio señalado por el auditado, estableciendo un plazo no mayor a 10 días hábiles. (Manual de Auditoria de Cumplimiento aprobado con RC N° 473-2014-CG).

Control interno.-

Se denomina control interno al conjunto de acciones, actividades, planes, políticas, normas, registros, organización, procedimientos y métodos incluyendo la actitud de las autoridades el personal organizado e instituido en cada entidad. (Ley N° 28716, Art. 3)

Eficacia.-

Del latín efficacĭa, la eficacia es la capacidad de alcanzar el efecto que espera o se desea tras la realización de una acción. No debe confundirse este concepto con el de eficiencia (del latín efficientĭa), que se refiere al uso racional de los medios para alcanzar un objetivo predeterminado (es decir, cumplir un objetivo con el mínimo de recursos disponibles y tiempo). (Pérez Porto y Merino, 2009).

Eficiencia.-

Eficiencia tiene su origen en el término latino *efficientia* y refiere a la habilidad de contar con algo o alguien para obtener un resultado. El concepto también suele ser equiparado con el de fortaleza o el de acción. http://definicion.de/ de Julián Pérez Porto y María Merino. Publicado: 2009.

Implementación.-

Una implementación es la ejecución u/o puesta en marcha de una idea programada, ya sea, de una aplicación informática, un plan, modelo científico, diseño especifico, estándar, algoritmo o política. Distíngase siempre el término implementación de implantación, puesto que una implantación se realiza de forma impuesta u obligatoria al usuario sin importar su opinión; en cambio en la implementación se involucra al usuario en el desarrollo de lo que se está realizando (Wikipedia diccionario libre).

Indicios de irregularidad.-

Es la acumulación de hechos que por su naturaleza corresponden a circunstancias de lo que es evidente, tan claro y perceptible que no se puede negar o poner en duda su fracaso respecto de la desviación de una realidad, producto de comparar con la norma o el estándar previsto. Hecho evidente, que no necesita explicación ciertos principios de la física se tienen por evidencias. (Wikipedia diccionario libre).

Normas de control interno.-

Constituyen lineamientos, criterios, métodos y disposiciones para la aplicación y regulación del control interno en las principales áreas de la actividad administrativa u operativa de las instituciones aplicación. Son criterios y prácticas de aceptación general, que se fundamentan en lineamientos y estándares de control. (Punto 3 de las Normas de Control Interno. Ley N° 28716).

Papeles de trabajo.-

Son los archivos o legajos que maneja el auditor y que contienen todos los documentos que sustentan su trabajo efectuado durante la auditoría.

Seguimiento y evaluación.-

El seguimiento y la evaluación (SyE) de las actividades de desarrollo tienen la finalidad de proveer un medio para aprender de la experiencia anterior, mejorar la prestación de

servicios, planificar y asignar recursos y demostrar los resultados para rendir cuentas a los interesados clave. Por lo tanto, esta publicación pretende fortalecer la concientización sobre las actividades de S y E y aclarar lo que implica. Se presenta una muestra de los instrumentos, métodos y enfoques, que incluyen ventajas y desventajas, costos, conocimientos y tiempo necesarios. Se consideran además los siguientes temas: indicadores de desempeño; enfoque del marco lógico; evaluación basada en la teoría; encuestas formales; métodos de evaluación inicial rápida; métodos participativos; estudios de seguimiento del gasto público; evaluación de los efectos; y análisis costo-beneficio y eficacia en función de los costos (Informe completo en español. Versión oficial del documento (PDF) Banco Mundial).

III MÉTODO

3.1. Tipo de investigación

3.1.1. Tipo

La investigación tiene las siguientes características:

a. **De acuerdo a su orientación: Aplicada.-** Procura brindar soluciones al problema constatado in situ.

b. **De acuerdo a la técnica de contrastación: Descriptiva.-** Es descriptiva porque el modelo de investigación establece la descripción y necesidad de exponer la mejora de la gestión informática a través de una metodología a plantearse.

c. **De acuerdo con la direccionalidad: Prospectiva.-** Porque tiene causas originadas en el pasado, que viene afectando el presente, es decir la gestión dentro del estado peruano y por ende el bienestar de la población.

d. **De acuerdo con el tipo de fuente de recolección de datos: Retrolectivo.-** La obtención existente de la información se recopila de los antecedentes históricos que han sido registrados por la Oficina de Control Interno en cada institución del estado Peruano.

e. **De acuerdo con la evolución del fenómeno estudiado: Transversal.-** Se toma en cuenta las variaciones de desplazamiento de la información en un determinado momento y los procesos desarrollados con la ejecución del presupuesto de la republica asignado a las instituciones del estado peruano.

f. **De acuerdo con la comparación de poblaciones: Comparativa.-** Porque se requiere dos estadios relacionales para contrastar la Hipotésis.

3.1.2. Nivel

Investigación de nivel III de Acción Aplicada y Predictiva; por qué utiliza conocimientos previos y presenta un nuevo aporte para el control y seguimiento de las actividades que se realizan en las entidades públicas con el dinero proveniente del erario nacional.

3.1.3. Diseño

El diseño de la presente investigación es Experimental (Experimental Puro), porque se manipulan deliberadamente una o más variables (independientes), con el objetivo de analizar su efecto sobre otras (dependientes), es decir la determinación de las relaciones de causa-efecto, en el marco de una situación controlada de sus elementos principales del cómo reaccionan. En líneas generales el trabajo de investigación comprenderá las siguientes etapas:

- Conocimiento de la entidad,
- Diseño, aprobación e implementación de estrategias para la mejora de la gestión de la Oficina de TI y
- Seguimiento, evaluación y retroalimentación.

Se analizó cuidadosamente la información obtenida y se interpretó mediante relaciones y argumentaciones teóricamente coherentes que ilustren correctamente la realidad estudiada.

3.2. Población y muestra

3.2.1. Población

El universo estará compuesto por 516 entidades que se encuentran ubicadas en el ámbito territorial del estado peruano.

3.2.2. Muestra

Para determinar el tamaño de la muestra se utilizó el método estadístico convencional relacionado al teorema de límite con un error admisible de estimación = 5%, y un nivel de

confianza de 95%; así como las probabilidades de éxito p = 0.4 y de fracaso q = 0.6; de tal manera que aplicando la siguiente fórmula:

$$n = \frac{Z^2 pqN}{Z^2 pq + (N-1)e} = \frac{Z^2 \sigma N}{Z^2 \sigma + (N-1)e} =$$

Siendo:

n = Tamaño muestral requerido

Z = Parámetro de la calidad del muestreo (usualmente Z=1.96) = 95% de confianza.

σ = Desviación estándar de la variable poblacional investigada. = (p*q).

e = Error admisible de la estimación.

p = Proporción de la población con cierto atributo (registro adecuado de datos)

q = Proporción de la población sin el atributo (registro inadecuado de datos)

N= Población representativa de 516 instituciones del estado peruano.

Aplicando la fórmula para determinar el tamaño de la muestra se obtiene:

$$n = \frac{(1.96)^2 (0.4)(0.6)(516)}{(1.96)^2 (0.4)(0.6) + (515)0.05} = 17.81 \cong 18 \text{ entidades públicas}$$

3.3. Operacionalización de variables

3.3.1. Estrategias de pruebas de hipótesis

Hipótesis principal nula

El diseño de una metodología dura para mejorar el sistema informático en las entidades públicas; NO mejoraría el control interno y por ende el uso de los recursos.

Hipótesis secundarias nulas

- La mejora de la organización e infraestructura de las oficinas de TI NO incide en la gestión pública y por ende en la consecución de los objetivos y metas.
- La gestión informática NO depende de la eficiencia en las adquisiciones, uso y mantenimiento de los recursos de TI.

- La vulnerabilidad del hardware y software instalado NO incide en la calidad de la información que procesan y divulgan las instituciones del estado peruano.

3.3.2. Operacionalización de variables e indicadores

Tabla 1

Operacionalización de variables e indicadores

HIPÓTESIS: El diseño de una metodología para mejorar el sistema informático en las entidades públicas; mejoraría el control interno y por ende el uso de los recursos		
VARIABLES	**INDICADORES**	
VI: Metodología para mejorar el sistema informático.	Eficiencia en el uso del presupuesto	Presupuesto ejecutado / Presupuesto programado para TI
	Cobertura del servicio	Nº. sistemas instalados / Nº. sistemas programados
	Personal que accede a la tecnología	Nº. de trabajadores con PC. / Total de trabajadores
	Presupuesto destinado a TI	Presupuesto programado para TI / Presupuesto total de la Entidad
	Acciones orientadas al ciudadano	Actividades orientadas al ciudadano / Total de actividades
	Obsolescencia del hardware	Tiempo de vida útil
	Mantenimiento del hardware	Mantenimiento preventivo ejecutado / Mantenimiento preventivo programado
VD1: Mejorar el control Interno	Eficacia en el cumplimiento de actividades	Actividades ejecutadas / Actividades programadas
VD2: Eficacia en el uso de los recursos	Eficiencia en el uso del presupuesto	Presupuesto ejecutado para TI / Presupuesto programado para TI
	Tiempos	Cantidad de proyectos no concluidos / Cantidad de proyectos concluidos fuera de plazo

3.4. Instrumentos

3.4.1. Selección

Para la ejecución del proyecto de investigación se utiliza como instrumento de recolección de datos: el cuestionario (formato de encuestas), entrevistas a autoridades de los diferentes niveles de mando y/o autoridad.

3.4.2. Validez de los instrumentos.

La validación se realizó en base al marco teórico de la categoría de "validez de contenido", utilizando el procedimiento de juicio de expertos calificados que determinaron la adecuación de los ítems de los respectivos instrumentos.

Se aplicó un cuestionario con escalas de Likert integrado por un total de (20) preguntas. Cabe acotar que se ha sistematizado la validez de contenido de las variables involucradas, lo cual ha sido validado por su aplicación en múltiples trabajos de investigación en distintas partes del mundo, apoyados por lo vertido en la mayoría de los informes de auditoría de control interno. En el presente estudio se aplicó procedimientos cuantitativos como las encuestas, entrevistas, la observación y las escalas de medición estadística y de actitudes.

3.5. Procedimientos

Se recopilo información mediante: entrevistas a los jefes de las Oficinas de Informática, revisión de los documentos internos solicitados en las acciones de control realizadas por el equipo de auditoría externa y de los publicados en la página de Transparencia del estado peruano. Una vez determinado el universo se seleccionó el tamaño de la muestra; teniendo en cuenta el cumplimiento de los criterios de representatividad, homogeneidad y aleatoriedad. Para la prueba de hipótesis se recopiló los datos de acuerdo a las variables y dimensiones.

A continuación se presenta una tabla conteniendo las técnicas e instrumentos que se utilizó.

3.5.1. Técnicas e Instrumentos de recolección de datos

Tabla 2

Técnicas e instrumentos

INVESTIGACION DE CAMPO	
TECNICAS	**INSTRUMENTOS**
La Observación directa: Sistemática o estructurada. Participante. Individual De grupo Usuarios Procedimientos.	 Diario de campo. Fichas de observación. Verificación Manual de procedimientos. Actividades de gestión.
La Observación indirecta:	Diario de Campo. Fichas de observación
Realización de Entrevistas: Estructuradas. Espontaneas. Dirigidas.	 Formato de entrevistas. Diario de campo. Grabaciones magnetofónicas.
Aplicación de Cuestionario: Abierto Cerrado.	 Formatos con preguntas de Cuestionario
INVESTIGACION NO EXPERIMENTAL	
TÉCNICAS	**INSTRUMENTOS**
Elaboración de modelos. Utilización de gabinetes. Seguimiento del comportamiento de las autoridades en los gastos. Seguimiento de las metodologías Seguimiento del comportamiento operativo de las entidades publicas Uso datos históricos.	Hojas estructuradas. Fichas de seguimiento. Computadoras de escritorio Presupuesto público Internet: página web.
INVESTIGACION DOCUMENTAL	
TÉCNICAS	**INSTRUMENTOS**
Revisión de: ❖ Libros. ❖ Revistas. ❖ Tesis ❖ Periódicos. ❖ Documentos ❖ Fotografías. ❖ Equipos de computo ❖ Internet.	 ❖ Fichas ❖ Cuadros sinópticos. ❖ Fotocopias. ❖ Diagramas. ❖ Computador. ❖ CD, disquete, casete ❖ Estadística inferencial

Nota: Elaboración propia

3.5.2. Diseño Estadístico

Para el diseño de la base de datos, el cuestionario se captura en Excel y traslada al software estadístico SPSS Ver. 25.0 para el tratamiento y análisis de los datos. Para determinar la confiabilidad del cuestionario se utilizó el coeficiente estadístico Alfa de Cronbach que nos permite medir la consistencia interna de la información obtenida; luego se trabajó con las variables paramétricas, cuyo análisis nos otorga evidencias para demostrar la aceptación o negación de la hipótesis estadística en función al estimador determinado.

3.6. Análisis de datos

Información en instituciones.- Se recopila y analiza la información estadística de las diversas entidades consideradas en el estudio de investigación.

Información de campo.- Obtención de datos de las entidades del estado peruano sobre: procesos, gestión, contabilidad y actividades desarrolladas.

Obtención de información sobre el sistema de trabajo que realizan los operadores de las entidades sobre gastos del año fiscal, documentos de los procesos, verificación de adquisiciones y/o servicios realizados.

Recopilación de información del área de informática de la entidad pública y desarrollo de los gastos en función al POI.

Encuestas a personas que laboran dentro de las entidades.

Encuestas a los operadores del uso sistema informático en cada entidad del estado seleccionado.

Entrevista a las autoridades.- Entrevistas a funcionarios de las entidades en estudio y al público usuario sobre la calidad del servicio, gestión del sistema informático, percepción ciudadana de la gestión, necesidad de información para mejorar los procesos de control, selección hecha de la muestra aleatoria.

Levantamiento de información histórica.- Se efectuará el levantamiento de información histórica con la finalidad de determinar la veracidad de los procesos y si estos están de acuerdo a ley del gasto público. Estos procedimientos se controlarán en diferentes periodos y etapas de los procesos de inversión o gasto previsto en el presupuesto público.

Actividades de procesamiento de datos y evaluación de la información.- Clasificación e interpretación de la información recopilada.

Determinación de planes y documentación requerida y empleada en la gestión de las entidades.

Determinar los requerimientos para mejorar la gestión.

Procesamiento de datos y análisis de la información.

Verificación de datos y actualización de procedimientos.

Verificación de procedimientos, retroalimentación y evaluación de la gestión.

3.7. Consideraciones éticas

El presente trabajo de investigación se alimenta de documentos internos emitidos por las entidades públicas estudiadas, revisión del portal de transparencia del estado peruano; así como de entrevistas y encuestas a los jefes de las oficinas de informática de la muestra.

Según lo estudiado por Rynolds, Levine y Skedsvold los principales problemas éticos que pueden originarse en este tipo de investigaciones se vinculan con: a) la invasión de la privacidad y la pérdida de la confidencialidad de la información brindada. (Hirsch A. 2013)

La «privacidad» y la «confidencialidad» son dos problemas éticos diferentes aunque relacionados. Para evitar invadir la privacidad de los encuestados o preguntados nos acercamos a ellos de forma respetuosa, explicando los objetivos de nuestro trabajo de investigación y tratando de no indagar más allá del límite moral o cultural impuesto por la persona entrevistada o por su grupo de pertenencia.

Con respecto a la confidencialidad, esta este es un principio siempre presente en las normas emitidas por la Contraloría general de la República, una de las últimas es las Normas Generales de Control Gubernamental, aprobada por Resolución de Contraloría Nº 295-2021-CG, de fecha 23 de diciembre de 2021, que en su capítulo segundo establece:

"II. NORMAS DE DESEMPEÑO PROFESIONAL

En el ejercicio de los servicios de control y servicios relacionados, el personal del SNC debe guiar su desempeño profesional por las normas de independencia, capacitación y competencia, diligencia profesional y confidencialidad; teniendo en cuenta los requisitos establecidos en la normativa vigente. El comportamiento ético del personal del SNC se rige de acuerdo a los correspondientes Códigos de Ética profesionales y de la función pública, así como la normativa emitida por la Contraloría."

3.8. Descripción de implementación metodológica

3.8.1. Diseño de la metodología dura

Esta metodología está orientada a realizar mejoras en el sistema de control interno de todas las dependencias públicas del estado peruano que realizan actividades y procesos relacionados con la gestión de las Oficinas de Tecnología de la Información – OTIs, propendiendo, de esta manera, a optimizar el proceso de auditoría externa. Los datos obtenidos de la propia entidad pública fueron cargados a un sistema modelador y de su proceso se obtuvo un diseño óptimo de control interno para cada entidad, en base a los cinco componentes: ambiente de control, evaluación de riesgos, actividades de control gerencial, información y comunicación y supervisión. La metodología comprende tres etapas que desarrollamos a

Etapa 1.- Conocimiento de la entidad.- La evaluación se realizó en base a los siguientes criterios:

Tabla 3

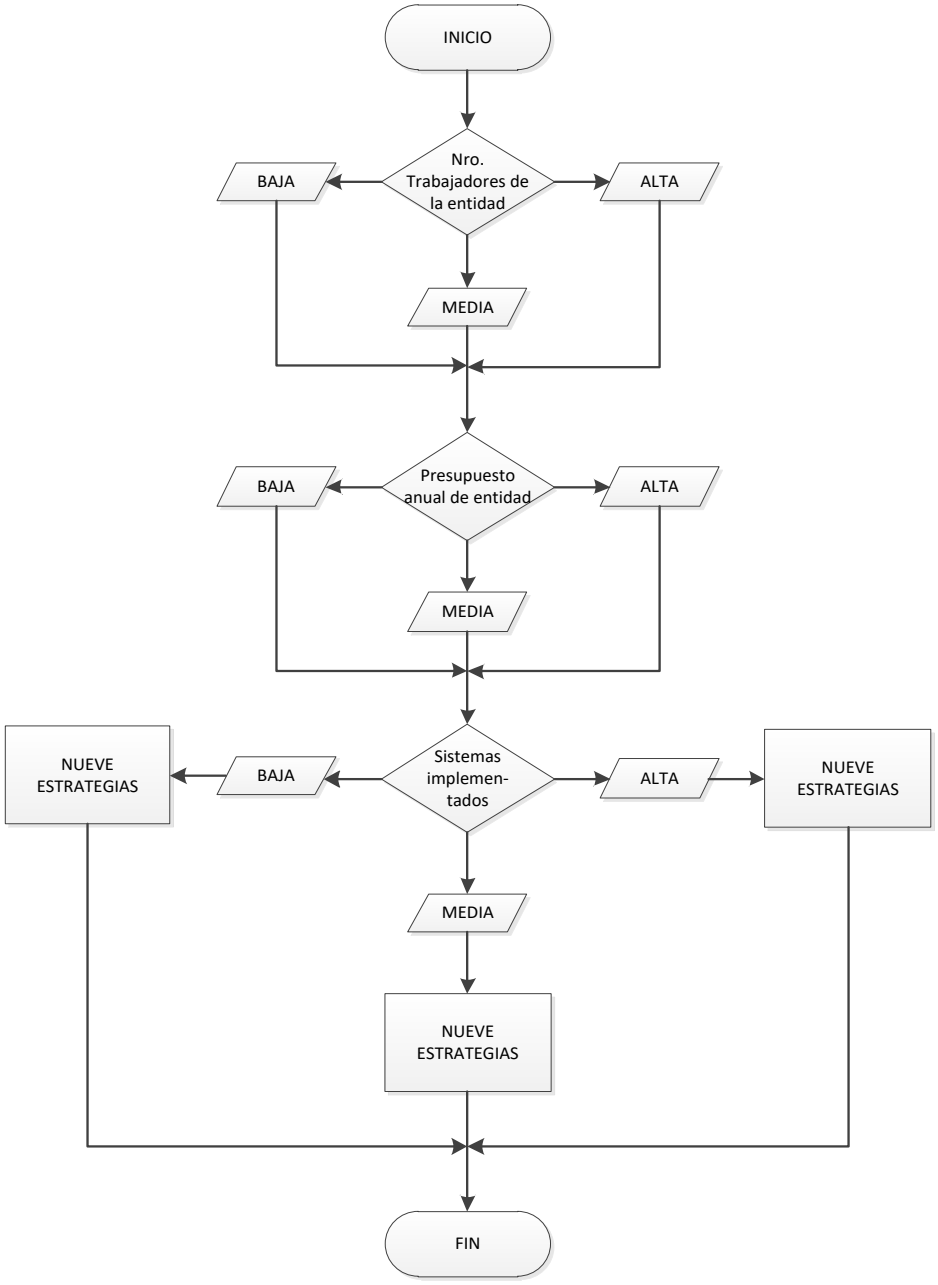
Criterios para evaluar la entidad

No.	CRITERIO	COMPLEJIDAD		
		BAJA	MEDIA	ALTA
1	Nº de trabajadores de la entidad	Menos de 199	De 200 a 999	De 1000 a más
2	Presupuesto anual de la entidad	Menos de un millón	De un millón a 10 millones	De 10 millones a más
3	Sistemas informáticos implementados	Menos de 5 sistemas	De 6 a 10 sistemas	DE 11 a más sistemas

Nota. Elaboración propia

Figura 04

Diagrama de flujo del procedimiento para evaluar la oficina de TI



Nota. Elaboración propia

Una vez determinadas las características de las entidades según su complejidad, se recopiló data anual, relacionada con:

- Adquisiciones de hardware, que comprende la cantidad servidores de red, computadoras, impresoras, proyectores, escáneres, equipos de protección eléctrica, switches de alta gama, cableado estructurado y equipos de seguridad perimetral.
- Adquisiciones de software, que comprende la cantidad de sistemas operativos para servidor, licencias CAL, sistemas operativos para estación de trabajo, Aplicativos para oficina, diseño, de seguridad (antivirus) y de mensajería.
- Mantenimiento de hardware y software, en lo que respecta a servidores, storage, estaciones de trabajo, base de datos y servicio de seguridad informática.

Además se aplicó, al jefe de la Oficina de Tecnologías de la Información, un Cuestionario de Control Interno con 107 preguntas (Ver Anexo C) que fueron evaluados por expertos y se elaboró una matriz de evaluación de riesgos (Ver Anexo D) con sus respectivos controles, seguimiento y retroalimentación, todo esto con la finalidad de evaluar la gestión de esta oficina.

Etapa 2.- Diseño e implementación de la organización optima de la oficina de TI para alcanzar los objetivos y metas.- Comprende el mejoramiento de la gestión de las 18 entidades de la muestra, mediante las siguientes actividades:

- Organización óptima de la Oficina de TI (ROF, MOF, CAP)
- Capacitación e inducción para obtener el ambiente de control ideal.
- Mejora de procesos de adquisición, uso y mantenimiento de los recursos de TI. e
- Implementación de normas de seguridad informática para el hardware y software instalado.

Etapa 3.- Seguimiento, Evaluación y Retroalimentación.- Con la finalidad de propender a la mejora continua de los procesos de la entidad.

IV. RESULTADOS

4.1. Implementación de las oficinas de informática

Tabla 4

Adquisiciones de hardware

ENTIDAD	Servidores	Compu-tadoras	Impresoras	Proyectores y escáneres	Equipos de protección eléctrica	Switch de alta gama	Cableado estructurado	Eq. para seguridad perimetral
SUNASA -Superintendencia Nacional de Salud	2	86	28	7	4			
SAT de Lima - Servicio de Administración Tributaria de Lima	4	125			2			
OSITRAN	1		4		3		1	
ONPE - Oficina Nacional de Procesos Electorales	9	45	7		31	10		5
INEN - Instituto Nacional de Enfermedades Neoplásicas	5	195			25	37		
MINJUS - Ministerio de Justicia	3	86	75	10				
JNE - Jurado Nacional de Elecciones	-	125	12	9				
GOREL - Gobierno Regional de Loreto	0	10	2					
GOREMAD - Gobierno Regional de Madre de Dios	2	123	3					
Servicio Nacional de Meteorología e Hidrología del Perú	12	22			7	9		
Municipalidad de La Victoria	1	39	11	10				
SISOL - Sistema Metropolitano De Solidaridad	0	284						
INVERMET - Fondo Metropolitano de Inversiones	1	59	3					
ICL - Instituto Catastral de Lima	0	40		4				
Municipalidad de Huancayo	1	28		4				
Municipalidad de Pasco	2	8						
EPS SEDAM Huancayo	1	26	4					
EPS SEDACAJ	O	6	9		2			1

Tabla 5

Adquisiciones de Software

ENTIDAD	SO para servidor	CAL para servidor	SO para estación de trabajo	Para oficina	Para diseño	Otros aplicativos	De seguridad (antivirus)	De mensajería
SUNASA -Superintendencia Nacional de Salud	2	30	86			4		
SAT de Lima - Servicio de Administración Tributaria de Lima	1	45	125			6		
OSITRAN- Organismo Supervisor de la Inversión en Infraestructura de Transporte	1					18		
ONPE - Oficina Nacional de Procesos Electorales	-				30			15
INEN - Instituto Nacional de Enfermedades Neoplásicas	195				15	1	600	
MINJUS - Ministerio de Justicia	14		170	180	5	6	2200	
JNE - Jurado Nacional de Elecciones	5	250		124	3	1		
GOREL - Gobierno Regional de Loreto	-							
GOREMAD - Gobierno Regional de Madre de Dios	-							
SENAMHI - Servicio Nacional de Meteorología e Hidrología del Perú	4		8	50				
Municipalidad de La Victoria	1		7					
SISOL - Sistema Metropolitano De Solidaridad	-							
INVERMET - Fondo Metropolitano de Inversiones	-				15	1		
ICL - Instituto Catastral de Lima	-					2		
Municipalidad de Huancayo	-		28					
Municipalidad de Pasco	-		8					
EPS SEDAM Huancayo	-		26					
EPS SEDACAJ	-	5	5	5				

Tabla 6

Mantenimiento de Hardware y Software

ENTIDAD	servidores	Storage	estaciones de trabajo	base de datos	Servicio de seguridad informática
SUNASA -Superintendencia Nacional de Salud	SI	SI	SI	SI	
SAT de Lima - Servicio de Administración Tributaria de Lima	SI	SI	SI	SI	
OSITRAN- Organismo Supervisor de la Inversión en Infraestructura de Transporte	SI		SI	SI	SI
ONPE - Oficina Nacional de Procesos Electorales	SI		SI	SI	
INEN - Instituto Nacional de Enfermedades Neoplásicas	SI		SI		SI
MINJUS - Ministerio de Justicia	SI	SI	SI		
JNE - Jurado Nacional de Elecciones	SI		SI		
GOREL - Gobierno Regional de Loreto	-		SI		
GOREMAD - Gobierno Regional de Madre de Dios	-		SI		
SENAMHI - Servicio Nacional de Meteorología e Hidrología del Perú	SI				
Municipalidad de La Victoria	-				
SISOL - Sistema Metropolitano De Solidaridad	-		SI		
INVERMET - Fondo Metropolitano de Inversiones	-				
ICL - Instituto Catastral de Lima	SI				
Municipalidad de Huancayo	-		SI		
Municipalidad de Pasco	-				
EPS SEDAM Huancayo	SI		SI		
EPS SEDACAJ	SI		SI		

Como se puede apreciar en las tres últimas tablas se han adquirido computadoras, equipos diversos, y otros de acuerdo a la necesidad de cada entidad en estudio, así como software para la implementación de ejecución presupuestal y control respectivo, cumpliendo con las indicaciones del plan a desarrollar para la auditoria del control interno informático, a fin de que conlleven a la optimización de los recursos del estado peruano, mejora de la gestión y disponibilidad de la información para agilizar la auditoría y control interno.

En lo que respecta al mantenimiento; el personal especializado aún se encuentra en proceso de capacitación, pero se viene avanzando para mantener el sistema activo, y el proceso de la seguridad informática; también se viene implementado el proceso, pero en las dos instituciones implementadas se viene llevando la evaluación y afinamiento de los procesos y generándose las actividades de control y seguridad respectiva, mejorándose los resultados como se van a visualizar en la presentación de tablas y análisis de resultados obtenidos.

4.2. Evaluación del instrumento por expertos

4.2.1. Contenido de ítems en el instrumento y valorización obtenida.

Tabla 7

Evaluación de los ítems del cuestionario de control interno

ITEMS		evaluación por expertos		
Nro.	P R E G U N T A	1ro.	2do.	3ro.
	A. MARCO ORGANIZATIVO:			
	A.1 Organización y personal de TI			
	La Oficina de Informática realiza las siguientes funciones:			
1	- Elabora políticas planes, normas y procedimientos de TICs?	1	1	0
2	- Análisis, desarrollo y mantenimiento de sistemas?	1	1	1
3	- Control de Calidad de los sistemas?	1	1	1
4	- Soporte Técnico a los usuarios?	1	1	1
5	- Seguridad Informática?	1	1	1
6	- Estas funciones están definidas en el ROF?	1	1	1
7	- El MOF describe las funciones de todo el personal considerado en el CAP?	1	1	1
8	- La gerencia asignó, por escrito, funciones al personal cuyo cargo no está considerado en el MOF?	1	1	1
9	- Se ha nombrado al Oficial de Seguridad de la Información?	1	1	1
	A.2 Planificación, políticas y procedimientos			
	La Oficina de Informática cuenta con los siguientes documentos de gestión:			
10	- Plan Estratégico de Tecnologías de la Información?	1	1	1
11	- Plan Estratégico de Gobierno Electrónico o similar?	1	1	1
12	- Plan Operativo Informático aprobado y remitido a la ONGEI-PCM?	1	1	1
13	- Evaluación del POI aprobado y remitido a la ONGEI-PCM?	1	1	1
14	- Políticas y normas de gestión de la seguridad de la información?	1	1	1
15	- Planes de formación y concientización en seguridad de TI?	1	1	1
16	- Plan o cronograma de mantenimiento preventivo de los equipos de cómputo?	1	1	1
17	- Procedimientos de gestión de riesgos de TI?	1	1	1
18	- Directivas para la gestión de las bases de datos de los sistemas que soportan los procesos administrativos.	1	1	1
19	- Normas internas sobre uso de internet y correo electrónico?	1	1	1
	B. GESTIÓN DE CAMBIOS EN SISTEMAS:			
	B.1 Adquisición de sistemas			

20	La entidad adquirió algún sistema para el manejo financiero y presupuestal con el presupuesto del ejercicio auditado?	1	1	1
21	La entidad adquirió otro tipo de software con el presupuesto del ejercicio auditado?	1	1	1
22	Elaboró el Informe Técnico Previo de Evaluación de Software antes de adquirir los programas antes mencionados?	1	1	1
	B.2 Desarrollo y mantenimiento de sistemas			
	Metodología de desarrollo de software:			
23	- Existe?	1	1	1
24	- Se aplica?	1	1	1
25	- Es suficiente?	0	1	1
26	El desarrollo o mantenimiento del software requiere:	1	1	1
27	- Autorización del Jefe del Usuario?	1	1	1
28	- Aprobación del Jefe de la OI?	1	1	1
29	- Aprobación de procedimientos de prueba de parte del usuario?	1	1	1
30	- Aprobación final del usuario antes de la puesta en marcha?	1	1	1
31	- Entornos físicos independientes para el desarrollo, pruebas y producción de software?	1	1	1
	B.3 Gestión de cambios en los sistemas			
32	La entidad cuenta con software administrador de cambios o de versiones?	1	1	1
33	Se documenta el mantenimiento de los sistemas, desde la solicitud hasta la aceptación final por parte del usuario?	1	1	1
34	Se generan o actualizan los manuales respectivos?	1	1	1
	C. OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN:			
	C.1 Operaciones TI			
35	La entidad cuenta con inventario de hardware actualizado?	1	1	1
36	La entidad cuenta con inventario de software actualizado?	1	1	1
37	Lleva una bitácora sobre las fallas y mantenimientos realizados a los equipos informáticos?	1	1	1
38	Existe software instalado en la entidad que no cuenta con licencias o autorizaciones de uso?	1	1	1
39	Se utiliza algún programa para detectar en la red la instalación de software ilegal o no autorizado?	1	1	1
	Se encuentran protegidos con software antivirus legal y actualizado:			
40	- Los servidores?	1	1	1
41	- Las estaciones de trabajo?	1	1	1
42	Se monitorea desde La Oficina de Informática las actualizaciones del antivirus?	1	1	1
	C.2 Seguridad física			
	Controles de acceso físico a la entidad			
43	- El local de la entidad está protegido contra robos?	1	1	1
44	- Se controla el ingreso de extraños al local?	1	1	1
45	- Existe un circuito cerrado de video vigilancia del local?	0	1	1
	Controles de acceso físico al centro de procesamiento de datos			
46	- El ambiente está diferenciado del resto de la infraestructura?	1	1	1

47	- Cuenta con un ambiente previo (zona de acceso y control)?	1	1	1
48	- Se accede mediante control biométrico?	1	1	1
49	- Se registra a las personas que acceden a la sala de servidores?	1	1	1
50	- Posee piso técnico o techo con placas suspendidas?	1	1	1
51	- Los gabinetes están dispuestos de manera adecuada?	1	1	1
52	- Los servidores están instalados dentro de sus racks respectivos?	1	1	1
53	- Existen servidores compatibles?	1	1	1
54	- Existen otros elementos no propios de una sala de servidores?	1	1	1
55	- Se han instalado cámaras de video o detectores de intrusos?	1	1	1
56	- Los equipos están conectadas a UPSs?.	1	1	1
57	- Los equipos están conectadas a circuitos con puesta a tierra?.	1	1	1
58	- Esta canalizada la transferencia de frio o calor?	1	1	1
59	- El ambiente cuenta con:	1	1	1
60	o Sistema contra incendios	1	1	1
61	o Detectores de inundación	1	1	1
62	o Detectores de humo	1	1	1
	C.3 Servicios contratados a terceros			
63	Los requerimientos de servicios de servicio de TI obedecen a una programación?	1	1	1
64	La Oficina de Informática controla el cumplimiento de los servicios contratados?	1	1	1
		1	1	1
	D. CONTROLES DE ACCESO A DATOS Y PROGRAMAS:			
	D.1 Protección de las redes y comunicaciones			
65	Existe interconexión entre locales?	1	1	1
	Cuenta con:			
66	- Acceso a internet (ancho de banda)	1	1	1
67	- Firewall o cortafuego físico	1	1	1
68	- Firewall Lógico	1	1	1
69	- Servidor de dominio	1	1	1
70	- Servidor proxy	1	1	1
71	- Switch core	1	1	1
72	- Switches de borde	1	1	1
73	- Switch de contingencia?	1	1	1
74	Los switches están instalados e gabinetes ventilados?	1	1	1
75	Las canaletas están en buen estado?	1	1	1
76	El cableado de la red de datos está certificado? CAT:	1	1	1
	D.2 Protección de gestión de usuarios			
77	Los usuarios fueron informados por escrito sobre las buenas prácticas de seguridad para la selección y uso de sus contraseñas?	1	1	1
78	Las sesiones de los usuarios se desactivan tras un periodo definido de inactividad?	1	1	1
	D.3 Mecanismos de identificación y autenticación			
79	El acceso al sistema es controlado con contraseña?	1	1	1
80	Están limitados los reintentos de acceso al sistema?	1	1	1

81	Se controla la existencia de datos faltantes?	1	1	1
82	Los procedimientos están estandarizados?	1	1	1
83	Se documenta el mantenimiento del sistema?	1	1	1
84	Los reportes impresos o la información mostrada en pantalla, identifican al usuario que envió el reporte?	1	1	1
85	Los reportes cuidan la correlación de los documentos emitidos?	1	1	1
86	Reciben los niveles gerenciales reportes para la toma de decisiones?	1	1	1
	D.4 Gestión de derechos de acceso			
87	La entidad adoptó una política de acceso a los sistemas, servicios informáticos y otros usos de la red?	1	1	1
88	Existen procedimientos para controlar la asignación de los derechos de acceso a los sistemas y demás servicios informáticos?	1	1	1
89	Está controlado el uso y asignación de privilegios para el acceso?	1	1	1
90	Mantiene un registro de todos los privilegios asignados?	1	1	1
91	Se controla por escrito la asignación de contraseñas?	1	1	1
92	- Está restringido el acceso al software de seguridad?	1	1	1
93	- Está restringido el acceso a los programas fuente?	1	1	1
94	- Está restringido el acceso a la base de datos?	1	1	1
95	- Está restringido el acceso a las copias de respaldo?	1	1	1
96	- Se realizan controles periódicos para asegurar que no se hayan presentado cambios no autorizados en los programas?	1	1	1
97	- Se han definido procedimientos de auditoría a la base de datos?	1	1	1
98	- Se utiliza filtros de correo electrónico para bloquear los mensajes?	1	1	1
99	- Se utiliza filtros web para controlar el acceso a internet solo a páginas autorizadas?	1	1	1
	E. CONTINUIDAD DE NEGOCIO (Servicios de TI)			
100	**E.1 Copias de seguridad**	1	1	1
101	La entidad cuenta con procedimientos, aprobados, para la generación y resguardo de copias de respaldo?	1	1	1
102	Los medios magnéticos con copias de respaldo son almacenados en lugares seguros?	1	1	1
103	Se almacenan una réplica de las copias de respaldo en otro local?	1	1	1
	E.2 Planes de continuidad			
	La Oficina de Informática cuenta con:			
104	- Normas internas sobre seguridad de la información en aplicación de la NTP ISO-IEC 17799-2007?	1	1	1
105	- Plan de Contingencias Informático?	1	1	1
106	- Pruebas periódicas del Plan de Contingencias Informático?	1	1	1
107	- Centros alternativos de procesamiento de datos	1	1	1

4.2.2. Formulación y evaluación de las preguntas por expertos

Tabla 8

Formulación y evaluación de las preguntas por expertos

			OBSERVADORES		
	N	ASPECTOS A CONSIDERAR	1	2	3
OBSERVACIONES	1	¿Las preguntas responden a los objetivos de la investigación?	1	1	1
	2	¿Las preguntas realmente miden las variables?	1	1	1
	3	¿El instrumento persigue el fin del objetivo general?	1	1	1
	4	¿El instrumento persigue los fines de los objetivos específicos?	1	1	1
	5	¿Las ideas planteadas son representativas del tema?	1	1	1
	6	¿Hay claridad en los ítems?	1	1	1
	7	¿Los ítems despiertan ambigüedad en sus respuestas?	1	1	1
	8	¿Las preguntas responden a un orden lógico?	1	1	1
	9	¿EL número de ítems por dimensiones es adecuado?	1	1	1
	10	¿El número de ítems por indicador es adecuado?	1	1	1
	11	¿La secuencia planteada es adecuada?	1	1	1
	12	¿Las preguntas deben ser reformuladas?	0	1	1
	13	¿Deben considerarse otros ítems?	1	1	1

38

CATEGORIAS:	
DE ACUERDO	1
EN DESACUERDO	0

Remplazando los valores en la fórmula: $P_0 = \frac{1}{N_c}\sum_{i=1}^{N_c}\frac{\sum_{k=1}^{K} X_{ik}(X_{ik}-1)}{J_i(J_i-1)}$

P_0 =	**0.948718**

Para determinar el valor esperado:

$$P_e = \frac{1}{N_c}\sum_{i=1}^{N_c}\frac{2}{J_i(J_i-1)}\frac{2}{J(J-1)}\sum_{m>I}^{J}\sum_{I=1}^{J}\sum_{k=1}^{K} P_j(k)P_m(k)$$

Reemplazando los valores de $P_j(k)$ en la fórmula:

$P_1(1)$	$P_2(1)$	$P_3(1)$
0.92307692	1	1
$P_1(2)$	$P_2(2)$	$P_3(2)$
0.07692308	0	0

$P_e =$	0.64459

Entonces: $$K = \frac{P_0 - P_e}{1 - P_e} = 0.85571$$

El valor obtenido nos indica que hay una buena correlación entre las preguntas formuladas. En la siguiente tabla y grafico se presenta la correlación de evaluación entre valorizaciones y que arroja aceptabilidad de correlación.

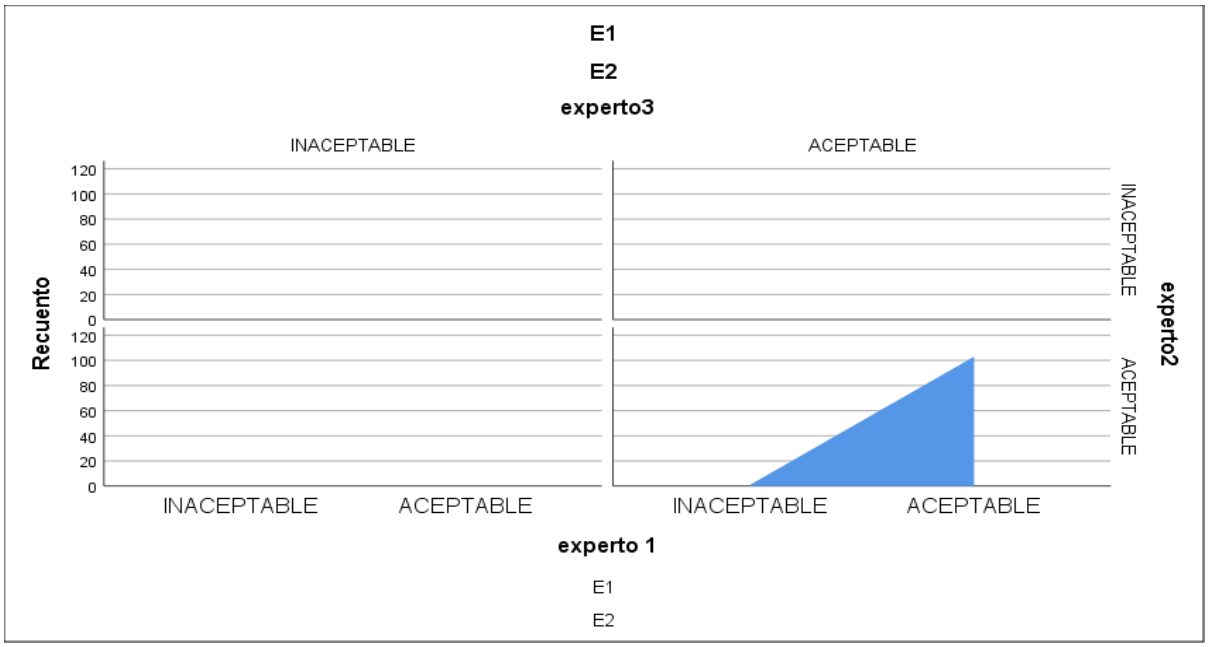
Tabla 9

Estadísticos descriptivos

	N	Mínimo	Máximo	Media	Desviación estándar
Experto 1	107	0	1	,99	,097
Experto 2	107	0	1	,98	,136
Experto 3	107	0	1	,99	,097
N válido (por lista)	107				

Figura 5

Análisis de aceptabilidad y correlación entre preguntas formuladas.



Nota. Elaboración propia

En la figura 05 se puede apreciar el nivel de aceptación de la formulación de preguntas formuladas luego de la evaluación del instrumento por expertos.

4.2.3. Prueba de normalidad.

Para realizar esta prueba se tomó en cuenta los datos de la encuesta antes de la aplicación tecnológica (pre) y luego de la ejecución de las indicaciones dadas (post), información que se puede observar en los resultados; con diferencias positivas y de mejora sustancial, así como el porcentaje para llegar al óptimo.

Tabla 10

Análisis de confiabilidad

	Media	Mínimo	Máx.	Rango	Máximo / Mínimo	Varianza	N de elementos
Medias de elemento	,988	,981	,991	,009	1,010	,000	3
Varianzas de elemento	,012	,009	,019	,009	1,981	,000	3

Tabla 11

Estadísticas de fiabilidad

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
-,036	-,037	3

Nota. El valor es negativo debido a una covarianza promedio negativa entre elementos. Esto viola los supuestos del modelo de fiabilidad. Podría desea comprobar las codificaciones de elemento. Elaboración propia.

Resultados de la pruebas de normalidad

a. Antes de la mejora

Tabla 12

Resumen de procesamiento de casos antes D

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
ANTES	95	88,8%	12	11,2%	107	100,0%

Nota. Elaboración propia

Tabla 13

Descriptivos antes D

			Estadístico	Desv. Error
ANTES	Media		48,6947	2,07513
	95% de intervalo de confianza para la media	Límite inferior	44,5745	
		Límite superior	52,8150	
	Media recortada al 5%		49,7690	
	Mediana		48,0000	
	Varianza		409,087	
	Desviación standard		20,22589	
	Mínimo		,00	
	Máximo		78,00	
	Rango		78,00	
	Rango intercuartil		25,00	
	Asimetría		-,762	,247
	Curtosis		,050	,490

Nota. Elaboración propia

Tabla 14

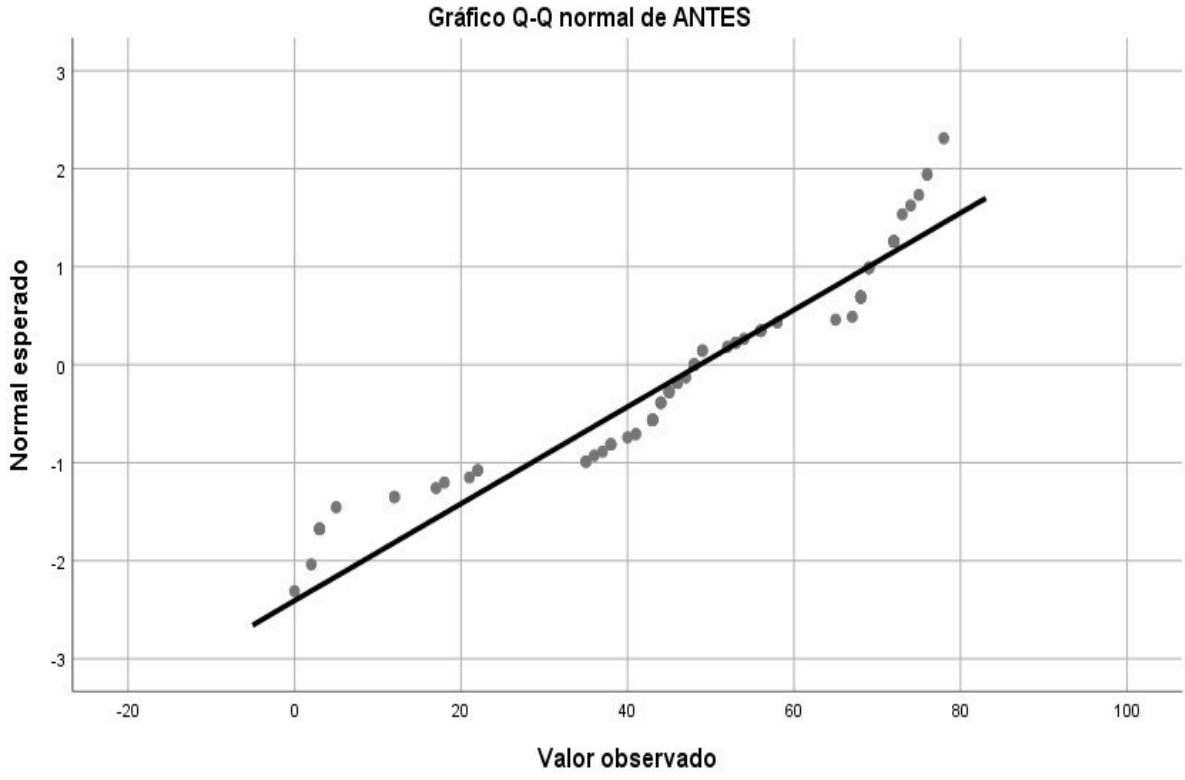
Pruebas de normalidad antes D

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
ANTES	,147	95	,000	,908	95	,000

Nota. a = Corrección de significación de Lilliefors. Elaboración propia

Figura 6

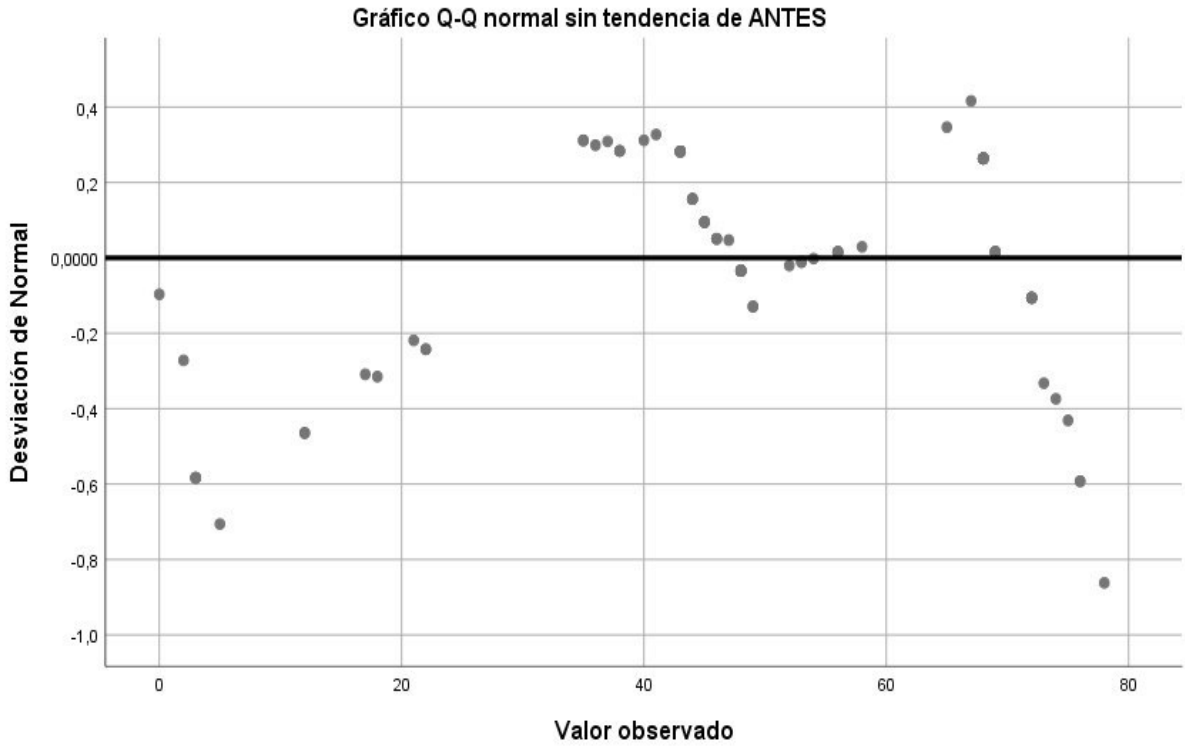
Gráfica de la distribución normal antes D



Nota. Elaboración propia

Figura 7

Grafica de la distribución observada



Nota. Elaboración propia

b. Después de la mejora

Tabla 15

Resumen de procesamiento de casos después D

	Casos					
	Válido		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
DESPUES	107	100,0%	0	0,0%	107	100,0%

Nota. Elaboración propia

Tabla 16

Datos Descriptivos después D

			Estadístico	Desv. Error
DESPUES	Media		87,2336	,48855
	95% de intervalo de confianza para la media	Límite inferior	86,2650	
		Límite superior	88,2022	
	Media recortada al 5%		88,1360	
	Mediana		89,0000	
	Varianza		25,539	
	Desviación standard		5,05364	
	Mínimo		60,00	
	Máximo		90,00	
	Rango		30,00	
	Rango intercuartil		3,00	
	Asimetría		-3,311	,234
	Curtosis		12,145	,463

Nota. Elaboración propia

Tabla 17

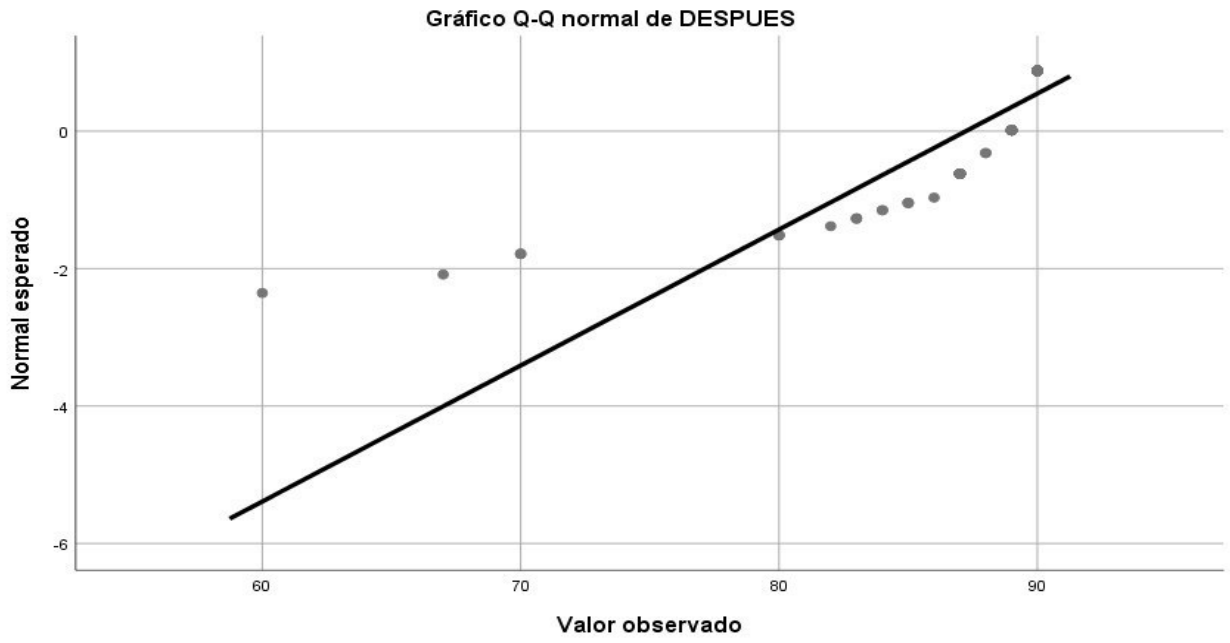
Pruebas de normalidad después D

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DESPUES	,313	107	,000	,561	107	,000

Nota. a = Corrección de significación de Lilliefors. Elaboración propia

Figura 8

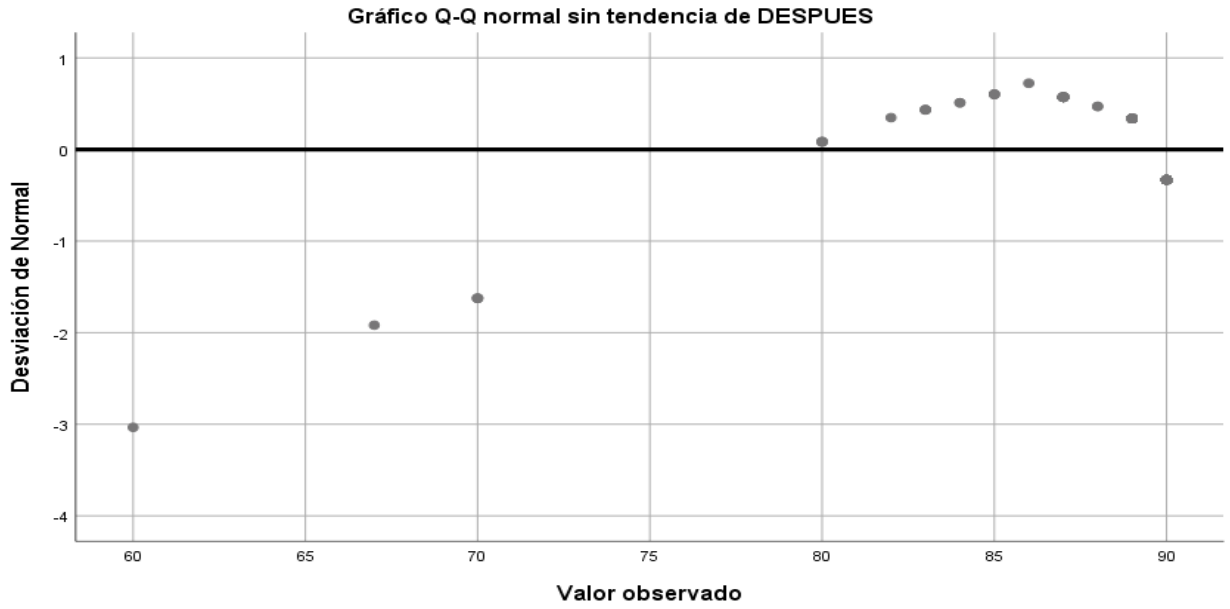
Grafica de la distribución normal después D



Nota. Elaboración propia

Figura 9

Gráfica de la distribución normal observada después D



Nota. Elaboración propia

Las distribuciones de los datos no siguen una distribución normal, como se puede apreciar en las gráficas anteriores. Por lo que se utilizará la ESTADISTICA NO PARAMETRICA. Obteniendo los siguientes resultados:

Tabla 18

Estadísticos descriptivos-análisis

	N	Media	Desv. Desviación	Mínimo	Máximo
ANTES	95	48,6947	20,22589	,00	78,00
DESPUES	107	87,2336	5,05364	60,00	90,00

Nota. Elaboración propia

Tabla 19

Utilizando estadígrafo de Wilcoxon (pruebas de rango)

		N	Rango promedio	Suma de rangos
DESPUES - ANTES	Rangos negativos	0[a]	,00	,00
	Rangos positivos	95[b]	48,00	4560,00
	Empates	0[c]		
	Total	95		

Nota. Elaboración propia

Tabla 20

Estadísticos de prueba[a]

Z	-8,465[b]
Sig. asintótica(bilateral)	,000

Nota. a = prueba de rangos con signo de Wilcoxon. b = Se basa en rangos negativos. Elaboración propia

Conclusión de la evaluación de distribución.- Del análisis de las tablas y gráficas se puede confirmar en líneas generales que la distribución es no paramétrica.

Tabla 21

Evaluación del consolidado de encuestas realizadas

instrumento con items utilizado	pos-test				pre-test				Diferen-cias		% diferenc. (pre y post)	al 100%=90 encuesta dos
P R E G U N T A	**SI**	**NO**	**N/A**	**N/R**	**SI**	**NO**	**N/A**	**N/R**	**si**	**no**		
A. MARCO ORGANIZATIVO:												
A.1 Organización y personal de TI												
La Oficina de Informática realiza las siguientes funciones:												
- Elabora políticas planes, normas y procedimientos de TICs?	**90**				**38**	**52**		**52**	52	-52	136.84	0.00
- Análisis, desarrollo y mantenimiento de sistemas?	**87**				**35**				52	0	148.57	3.33
- Control de Calidad de los sistemas?	**80**	**10**		**10**	**22**	**68**		**68**	58	-58	263.64	11.11
- Soporte Técnico a los usuarios?	**86**				**40**				46		115.00	4.44
- Seguridad Informática?	**80**				**54**				26		48.15	11.11
- Estas funciones están definidas en el ROF?	**90**				**72**				18		25.00	0.00
- El MOF describe las funciones de todo el personal considerado en el CAP?	**90**				**45**	**45**		**45**	45	-45	100.00	0.00
- La gerencia asignó, por escrito, funciones al personal cuyo cargo no está considerado en el MOF?	**90**				**56**				34		60.71	0.00
- Se ha nombrado al Oficial de Seguridad de la Información?	**90**				**17**	**73**		**73**	73	-73	429.41	0.00
A.2 Planificación, políticas y procedimientos												
La Oficina de Informática cuenta con los siguientes documentos de gestión:												
- Plan Estratégico de Tecnologías de la Información?	**85**				**41**	**49**		**49**	44	-49	107.32	5.56

- Plan Estratégico de Gobierno Electrónico o similar?	70				52	38		38	18	-38	34.62	22.22
- Plan Operativo Informático aprobado y remitido a la ONGEI-PCM?	90				45				45	0	100.00	0.00
- Evaluación del POI aprobado y remitido a la ONGEI-PCM?	89				45				44	0	97.78	1.11
- Políticas y normas de gestión de la seguridad de la información?	88				45				43	0	95.56	2.22
- Planes de formación y concientización en seguridad de TI?	70	20		20	53	37		37	17	-17	32.08	22.22
- Plan o cronograma de mantenimiento preventivo de los equipos de cómputo?	90				36				54	0	150.00	0.00
- Procedimientos de gestión de riesgos de TI?	80	10		10	75	25		25	5	-15	6.67	11.11
- Directivas para la gestión de las bases de datos de los sistemas que soportan los procesos administrativos.	90				68				22		32.35	0.00
- Normas internas sobre uso de internet y correo electrónico?	87				38				49		128.95	3.33
B. GESTIÓN DE CAMBIOS EN SISTEMAS:												
B.1 Adquisición de sistemas												
La entidad adquirió algún sistema para el manejo financiero y presupuestal con el presupuesto del ejercicio auditado?	70	20		20	44	46		46	26	-26	59.09	22.22
La entidad adquirió otro tipo de software con el presupuesto del ejercicio auditado?	60				35				25		71.43	33.33
Elaboró el Informe Técnico Previo de Evaluación de Software antes de adquirir los programas antes mencionados?	90				47				43		91.49	0.00
B.2 Desarrollo y mantenimiento de sistemas												
Metodología de desarrollo de software:												
- Existe?	87				3	87		87	84	-87	2800.00	3.33
- Se aplica?	84				3	87		87	81	-87	2700.00	6.67
- Es suficiente?	67				3	87		87	64	-87	2133.33	25.56
El desarrollo o mantenimiento del software requiere:												
- Autorización del Jefe del Usuario?	90				72				18	0	25.00	0.00
- Aprobación del Jefe de la OI?	90				72				18	0	25.00	0.00
- Aprobación de procedimientos de prueba de parte del usuario?	90				72				18	0	25.00	0.00
- Aprobación final del usuario antes de la puesta en marcha?	90				72				18	0	25.00	0.00

- Entornos físicos independientes para el desarrollo, pruebas y producción de software?	85	5		5	3	87		87	82	-82	2733.33	5.56
B.3 Gestión de cambios en los sistemas												
La entidad cuenta con software administrador de cambios o de versiones?	87				2	88		88	85	-88	4250.00	3.33
Se documenta el mantenimiento de los sistemas, desde la solicitud hasta la aceptación final por parte del usuario?	87				68				19	0	27.94	3.33
Se generan o actualizan los manuales respectivos?	88				68				20	0	29.41	2.22
C. OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN:												
C.1 Operaciones TI												
La entidad cuenta con inventario de hardware actualizado?	90				69				21	0	30.43	0.00
La entidad cuenta con inventario de software actualizado?	90				69				21	0	30.43	0.00
Lleva una bitácora sobre las fallas y mantenimientos realizados a los equipos informáticos?	90				43	47		47	47	-47	109.30	0.00
Existe software instalado en la entidad que no cuenta con licencias o autorizaciones de uso?	90	0		0	43	47		47	47	-47	109.30	0.00
Se utiliza algún programa para detectar en la red la instalación de software ilegal o no autorizado?	90	0		0	43	47		47	47	-47	109.30	0.00
Se encuentran protegidos con software antivirus legal y actualizado:												
- Los servidores?	90				69				21		30.43	0.00
- Las estaciones de trabajo?	89				69				20		28.99	1.11
Se monitorea desde La Oficina de Informática las actualizaciones del antivirus?	87				48				39		81.25	3.33
C.2 Seguridad física												
Controles de acceso físico a la entidad												
- El local de la entidad está protegido contra robos?	90				49				41		83.67	0.00
- Se controla el ingreso de extraños al local?	90				73				17		23.29	0.00
- Existe un circuito cerrado de video vigilancia del local?	87				0	90		90	87	-90		3.33
Controles de acceso físico al centro de procesamiento de datos												
- El ambiente está diferenciado del resto de la infraestructura?	90				72				18		25.00	0.00
- Cuenta con un ambiente previo (zona de acceso y control)?	90				67				23		34.33	0.00

- Se accede mediante control biométrico?	90				12	78		M	78	-78	650.00	0.00
- Se registra a las personas que acceden a la sala de servidores?	90				56				34		60.71	0.00
- Posee piso técnico o techo con placas suspendidas?		0		0		78		M	0	-78		
- Los gabinetes están dispuestos de manera adecuada?	87				49				38		77.55	3.33
- Los servidores están instalados dentro de sus racks respectivos?	89				46				43		93.48	1.11
- Existen servidores compatibles?	87				68				19		27.94	3.33
- Existen otros elementos no propios de una sala de servidores?	87	0			78	12			9	-12	11.54	3.33
- Se han instalado cámaras de video o detectores de intrusos?	87				18	72		A	69	-72	383.33	3.33
- Los equipos están conectadas a UPSs?.	89				56				33	0	58.93	1.11
- Los equipos están conectadas a circuitos con puesta a tierra?.	89				56				33	0	58.93	1.11
- Esta canalizada la transferencia de frio o calor?	89	0		0	53	37		37	36	-37	67.92	1.11
- El ambiente cuenta con:												
o Sistema contra incendios	89				38				51	0	134.21	1.11
o Detectores de inundación	83	5		5	12	78		78	71	-73	591.67	7.78
o Detectores de humo	87				5	85		85	82	-85	1640.00	3.33
C.3 Servicios contratados a terceros												
Los requerimientos de servicios de servicio de TI obedecen a una programación?	89				65				24		36.92	1.11
La Oficina de Informática controla el cumplimiento de los servicios contratados?	90				56				34		60.71	0.00
D. CONTROLES DE ACCESO A DATOS Y PROGRAMAS:												
D.1 Protección de las redes y comunicaciones												
Existe interconexión entre locales?	90				74				16		21.62	0.00
Cuenta con:												
- Acceso a internet (ancho de banda)	90				68				22		32.35	0.00
- Firewall o cortafuego físico	90				68				22		32.35	0.00
- Firewall Lógico		0		0		0		0				
- Servidor de dominio	90				22	68		68	68	-68	309.09	0.00
- Servidor proxy	90				68				22	0	32.35	0.00

- Switch core	90				68				22	0	32.35	0.00
- Switches de borde	90				68				22	0	32.35	0.00
- Switch de contingencia?	90				46	44		44	44	-44	95.65	0.00
Los switches están instalados e gabinetes ventilados?	90				68				22		32.35	0.00
Las canaletas están en buen estado?	90				68				22		32.35	0.00
El cableado de la red de datos está certificado? CAT:	84	0		0	34	56		56	50	-56	147.06	6.67
D.2 Protección de gestión de usuarios												
Los usuarios fueron informados por escrito sobre las buenas prácticas de seguridad para la selección y uso de sus contraseñas?	87				58				29		50.00	3.33
Las sesiones de los usuarios se desactivan tras un periodo definido de inactividad?	82				57				25		43.86	8.89
D.3 Mecanismos de identificación y autenticación									0			
El acceso al sistema es controlado con contraseña?	90				76				14		18.42	0.00
Están limitados los reintentos de acceso al sistema?	90				76				14		18.42	0.00
Se controla la existencia de datos faltantes?	87	0		0	44	46		46	43	-46	97.73	3.33
Los procedimientos están estandarizados?	87				44	46		B	43	-46	97.73	3.33
Se documenta el mantenimiento del sistema?	89				68				21		30.88	1.11
Los reportes impresos o la información mostrada en pantalla, identifican al usuario que envió el reporte?	83	5		5	21	69		69	62	-64	295.24	7.78
Los reportes cuidan la correlación de los documentos emitidos?	89				72				17		23.61	1.11
Reciben los niveles gerenciales reportes para la toma de decisiones?	89				72				17		23.61	1.11
D.4 Gestión de derechos de acceso												
La entidad adoptó una política de acceso a los sistemas, servicios informáticos y otros usos de la red?	89				48				41		85.42	1.11
Existen procedimientos para controlar la asignación de los derechos de acceso a los sistemas y demás servicios informáticos?	89				44	56		56	45	-56	102.27	1.11
Está controlado el uso y asignación de privilegios para el acceso?	89				48				41		85.42	1.11
Mantiene un registro de todos los privilegios asignados?	89				48				41		85.42	1.11
Se controla por escrito la asignación de contraseñas?	89				46				43		93.48	1.11
- Está restringido el acceso al software de seguridad?	89				48				41		85.42	1.11
- Está restringido el acceso a los programas fuente?	89				48				41		85.42	1.11

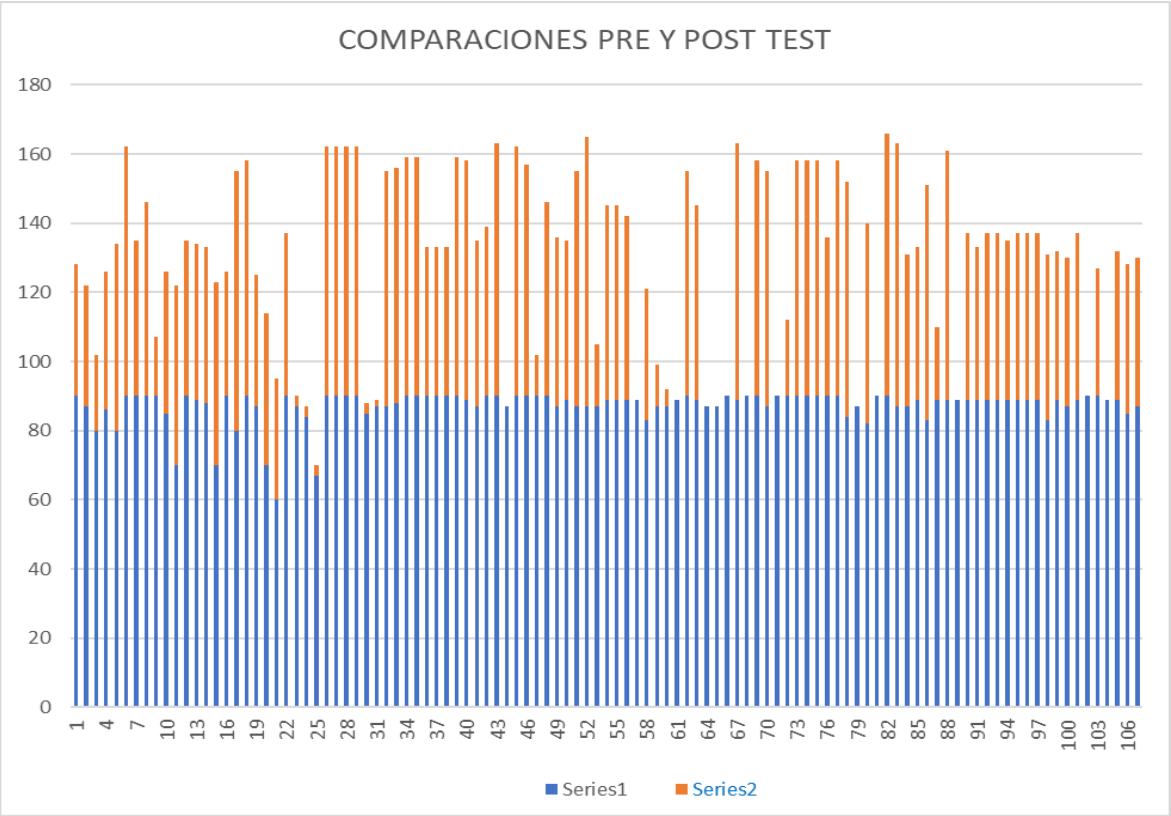
- Está restringido el acceso a la base de datos?	89				48				41		85.42	1.11
- Está restringido el acceso a las copias de respaldo?	89				48				41		85.42	1.11
- Se realizan controles periódicos para asegurar que no se hayan presentado cambios no autorizados en los programas?	83	5		5	43	47		47	40	-42	93.02	7.78
- Se han definido procedimientos de auditoría a la base de datos?	89				43	47		47	46	-47	106.98	1.11
- Se utiliza filtros de correo electrónico para bloquear los mensajes?	87				48				39		81.25	3.33
- Se utiliza filtros web para controlar el acceso a internet solo a páginas autorizadas?	89				48				41		85.42	1.11
E. CONTINUIDAD DE NEGOCIO (Servicios de TI)												
E.1 Copias de seguridad												
La entidad cuenta con procedimientos, aprobados, para la generación y resguardo de copias de respaldo?	90				37				53		143.24	0.00
Los medios magnéticos con copias de respaldo son almacenados en lugares seguros?	90				37				53		143.24	0.00
Se almacenan una réplica de las copias de respaldo en otro local?									53		143.24	0.00
E.2 Planes de continuidad												
La Oficina de Informática cuenta con:												
- Normas internas sobre seguridad de la información en aplicación de la NTP ISO-IEC 17799-2007?	89				43	47		47	46	-47	106.98	1.11
- Plan de Contingencias Informático?	89				43	47		47	46	-47	106.98	1.11
- Pruebas periódicas del Plan de Contingencias Informático?	85	5		5	43	47		47	42	-42	97.67	5.56
- Centros alternativos de procesamiento de datos	87	3		3	43	47		47	44	-44	102.33	3.33

Nota. Elaboración propia

Análisis y descripción de los resultados.- En la tabla 21, se puede apreciar que la metodología implementada ha generado satisfacción en los usuarios y mejora en los resultados, todos los ítems considerados en el instrumento de medición han dado resultados positivos, llegando en algunos casos a una mejora del 100%, también la relación entre lo que se venía haciendo y lo que se hace después de la implementación ha mejorado en algunos actividades doce veces más, como en otros ha superado en veintidós (22) veces más las actividades que se habían realizado antes de implementar la metodología. Por lo que se puede deducir que la mejora ha sido sustancial después de implementación de la metodología, como también se puede apreciar la figura 10.

Figura 10

Comparaciones de resultados del pre(azul) y pos-test(rojo).



Nota. Elaboración propia

4.2.4. Planteamiento y evaluación de las Hipótesis estadísticas:

1ra. HIPOTESIS ESPECÍFICA

Ha: La mejora de la organización e infraestructura de las oficinas de TI mediante la implementación de una metodología dura contribuiría en alcanzar los objetivos y metas del Control interno. ($\mathbf{X} > \mathbf{X_1}$).

Ho: La mejora de la organización e infraestructura de las oficinas de TI mediante la implementación de una metodología dura NO contribuiría en alcanzar los objetivos y metas del Control interno. ($\mathbf{X} < \mathbf{X_1}$).

2da. HIPOTESIS ESPECÍFICA

Ha : Las adquisiciones, uso y mantenimiento de los recursos de TI, con la implementación de una metodología, mejoraría la gestión de la entidad pública. ($\mathbf{X} > \mathbf{X_1}$).

Ho: Las adquisiciones, uso y mantenimiento de los recursos de TI, con la implementación de una metodología, no mejoraría la gestión de la entidad pública. ($\mathbf{X} < \mathbf{X_1}$).

3ra. HIPOTESIS ESPECÍFICA

Ha: El hardware y software instalado mediante la implementación de una metodología cumple con las normas de seguridad Informática. ($\mathbf{X} > \mathbf{X_1}$).

Ho: El hardware y software instalado mediante la implementación de una metodología no cumple con las normas de seguridad Informática. ($\mathbf{X} < \mathbf{X_1}$).

Análisis de datos para la 1ra. Hipótesis específica:

Tabla 22

Resultados de respuestas ítem´s 1:

instrumento con ítems utilizados	pos-test				pre-test				Diferencias		% diferenc (pre y post)	al 100%=90 encuestados
P R E G U N T A	**SI**	**NO**	**N/A**	**N/R**	**SI**	**NO**	**N/A**	**N/R**	**si**	**no**		
A. MARCO ORGANIZATIVO:												
A.1 Organización y personal de TI												
La Oficina de Informática realiza las siguientes funciones:												
- Elabora políticas planes, normas y procedimientos de TICs?	90				38	52		52	52	-52	136.84	0.00
- Análisis, desarrollo y mantenimiento de sistemas?	87				35				52	0	148.57	3.33
- Control de Calidad de los sistemas?	80	10		10	22	68		68	58	-58	263.64	11.11
- Soporte Técnico a los usuarios?	86				40				46		115.00	4.44
- Seguridad Informática?	80				54				26		48.15	11.11
- Estas funciones están definidas en el ROF?	90				72				18		25.00	0.00
- El MOF describe las funciones de todo el personal considerado en el CAP?	90				45	45		45	45	-45	100.00	0.00
- La gerencia asignó, por escrito, funciones al personal cuyo cargo no está considerado en el MOF?	90				56				34		60.71	0.00
- Se ha nombrado al Oficial de Seguridad de la Información?	90				17	73		73	73	-73	429.41	0.00
A.2 Planificación, políticas y procedimientos												
La Oficina de Informática cuenta con los siguientes documentos de gestión:												
- Plan Estratégico de Tecnologías de la Información?	85				41	49		49	44	-49	107.32	5.56
- Plan Estratégico de Gobierno Electrónico o similar?	70				52	38		38	18	-38	34.62	22.22
- Plan Operativo Informático aprobado y remitido a la ONGEI-PCM?	90				45				45	0	100.00	0.00

-	Evaluación del POI aprobado y remitido a la ONGEI-PCM?	89				45				44	0	97.78	1.11
-	Políticas y normas de gestión de la seguridad de la información?	88				45				43	0	95.56	2.22
-	Planes de formación y concientización en seguridad de TI?	70	20		20	53	37		37	17	-17	32.08	22.22
-	Plan o cronograma de mantenimiento preventivo de los equipos de cómputo?	90				36				54	0	150.00	0.00
-	Procedimientos de gestión de riesgos de TI?	80	10		10	75	25		25	5	-15	6.67	11.11
-	Directivas para la gestión de las bases de datos de los sistemas que soportan los procesos administrativos.	90				68				22		32.35	0.00
-	Normas internas sobre uso de internet y correo electrónico?	87				38				49		128.95	3.33

Nota. *Elaboración propia*

En la figura 10, se puede observar que los resultados superan en altos porcentajes el incremento de mejora en las actividades de organización, por lo que se puede decir que se acepta la Hipotésis del investigador, y se demuestra que se han alcanzado los objetivos y metas del control interno.

Tabla 23

Correlaciones NO paramétricas

			antes	después
Rho de Spearman	antes	Coeficiente de correlación	1,000	-,086
		Sig. (bilateral)	.	,725
		N	19	19
	después	Coeficiente de correlación	-,086	1,000
		Sig. (bilateral)	,725	.
		N	19	19

Figura 11

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	La distribución de antes es normal con la media 85 y la desviación estándar 6,483.	Prueba de Kolmogorov-Smirnov para una muestra	,006[1]	Rechazar la hipótesis nula.
2	La distribución de despues es normal con la media 48 y la desviación estándar 15,056.	Prueba de Kolmogorov-Smirnov para una muestra	,200[1,2]	Retener la hipótesis nula.
3	La distribución de diferencias es normal con la media 39 y la desviación estándar 17,274.	Prueba de Kolmogorov-Smirnov para una muestra	,018[1]	Rechazar la hipótesis nula.

Nota. Se muestran significaciones asintóticas. El nivel de significación es de ,006. 1=Lilliefors corregida. 2=Se trata de un límite inferior a la significación real

Se acepta la Hipótesis del investigador y se rechaza la hipótesis nula, de acuerdo a los resultados obtenidos con el **SPSS** versión 25.00., como se puede visualizar en la figura 11.

Análisis de datos para la 2da. Hipótesis específica:

Tabla 24

Resultados de respuestas ítem´s2

instrumento con ítems utilizados	post-test				pre-test				Diferencias		% diferenc (pre y post)	al 100%=90 encuestados
P R E G U N T A	**SI**	**NO**	**N/A**	**N/R**	**SI**	**NO**	**N/A**	**N/R**	**si**	**no**		
B. **GESTIÓN DE CAMBIOS EN SISTEMAS:**												
B.1 Adquisición de sistemas												
La entidad adquirió algún sistema para el manejo financiero y presupuestal con el presupuesto del ejercicio auditado?	70	20		20	44	46		46	26	-26	59.09	22.22
La entidad adquirió otro tipo de software con el presupuesto del ejercicio auditado?	60				35				25		71.43	33.33
Elaboró el Informe Técnico Previo de Evaluación de Software antes de adquirir los programas antes mencionados?	90				47				43		91.49	0.00
B.2 Desarrollo y mantenimiento de sistemas												
Metodología de desarrollo de software:												
- Existe?	87				3	87		87	84	-87	2800.00	3.33
- Se aplica?	84				3	87		87	81	-87	2700.00	6.67
- Es suficiente?	67				3	87		87	64	-87	2133.33	25.56
El desarrollo o mantenimiento del software requiere:												
- Autorización del Jefe del Usuario?	90				72				18	0	25.00	0.00
- Aprobación del Jefe de la OI?	90				72				18	0	25.00	0.00
- Aprobación de procedimientos de prueba de parte del usuario?	90				72				18	0	25.00	0.00
- Aprobación final del usuario antes de la puesta en marcha?	90				72				18	0	25.00	0.00
- Entornos físicos independientes para el desarrollo, pruebas y producción de software?	85	5		5	3	87		87	82	-82	2733.33	5.56
B.3 Gestión de cambios en los sistemas												

La entidad cuenta con software administrador de cambios o de versiones?	87				2	88		88	85	-88	4250.00	3.33
Se documenta el mantenimiento de los sistemas, desde la solicitud hasta la aceptación final por parte del usuario?	87				68				19	0	27.94	3.33
Se generan o actualizan los manuales respectivos?	88				68				20	0	29.41	2.22
C. **OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN:**												
C.1 Operaciones TI												
La entidad cuenta con inventario de hardware actualizado?	90				69				21	0	30.43	0.00
La entidad cuenta con inventario de software actualizado?	90				69				21	0	30.43	0.00
Lleva una bitácora sobre las fallas y mantenimientos realizados a los equipos informáticos?	90				43	47		47	47	-47	109.30	0.00
Existe software instalado en la entidad que no cuenta con licencias o autorizaciones de uso?	90	0		0	43	47		47	47	-47	109.30	0.00
Se utiliza algún programa para detectar en la red la instalación de software ilegal o no autorizado?	90	0		0	43	47		47	47	-47	109.30	0.00
Se encuentran protegidos con software antivirus legal y actualizado:												
- Los servidores?	90				69				21		30.43	0.00
- Las estaciones de trabajo?	89				69				20		28.99	1.11
Se monitorea desde La Oficina de Informática las actualizaciones del antivirus?	87				48				39		81.25	3.33
C.2 Seguridad física												
Controles de acceso físico a la entidad												
- El local de la entidad está protegido contra robos?	90				49				41		83.67	0.00
- Se controla el ingreso de extraños al local?	90				73				17		23.29	0.00
- Existe un circuito cerrado de video vigilancia del local?	87				0	90		90	87	-90		3.33
Controles de acceso físico al centro de procesamiento de datos												
- El ambiente está diferenciado del resto de la infraestructura?	90				72				18		25.00	0.00
- Cuenta con un ambiente previo (zona de acceso y control)?	90				67				23		34.33	0.00
- Se accede mediante control biométrico?	90				12	78		M	78	-78	650.00	0.00
- Se registra a las personas que acceden a la sala de servidores?	90				56				34		60.71	0.00

- Posee piso técnico o techo con placas suspendidas?		0		0		78		M	0	-78		
- Los gabinetes están dispuestos de manera adecuada?	87				49				38		77.55	3.33
- Los servidores están instalados dentro de sus racks respectivos?	89				46				43		93.48	1.11
- Existen servidores compatibles?	87				68				19		27.94	3.33
- Existen otros elementos no propios de una sala de servidores?	87	0			78	12			9	-12	11.54	3.33
- Se han instalado cámaras de video o detectores de intrusos?	87				18	72		A	69	-72	383.33	3.33
- Los equipos están conectadas a UPSs?.	89				56				33	0	58.93	1.11
- Los equipos están conectadas a circuitos con puesta a tierra?.	89				56				33	0	58.93	1.11
- Esta canalizada la transferencia de frio o calor?	89	0		0	53	37		37	36	-37	67.92	1.11
- El ambiente cuenta con:												
o Sistema contra incendios	89				38				51	0	134.21	1.11
o Detectores de inundación	83	5		5	12	78		78	71	-73	591.67	7.78
○ Detectores de humo	87				5	85		85	82	-85	1640.00	3.33
C.3 Servicios contratados a terceros												
Los requerimientos de servicios de servicio de TI obedecen a una programación?	89				65				24		36.92	1.11
La Oficina de Informática controla el cumplimiento de los servicios contratados?	90				56				34		60.71	0.00

Nota. *Elaboración propia*

Tabla 25

Prueba de Kolmogorov-Smirnov para la muestra

		H2DIFERENCIAS
N		42
Parámetros normales[a,b]	Media	40,5714
	Desv. Desviación	23,84211
Máximas diferencias extremas	Absoluto	,158
	Positivo	,158
	Negativo	-,138
Estadístico de prueba		,158
Sig. asintótica(bilateral)		,010[c]

Nota. a = La distribución de prueba es normal. b = Se calcula a partir de datos. C. Corrección de significación de Lilliefors

Se puede visualizar en la tabla 24, que los resultados indican que se ha incrementado en un alto porcentaje. La tabla 25 contiene los detalles descriptivos del procesamiento de datos, donde se refleja las mejoras en las actividades, con la adquisición, uso y mantenimiento de los recursos de TI, con lo que se concluye que se acepta la Hipótesis del investigador; por lo tanto; la implementación de la metodología aplicada mejora la gestión de la entidad pública.

Análisis de datos para la 3ra. Hipótesis específica:

Tabla 26

Resultados de respuestas ítem´s 3

instrumento con ítems utilizados	pos-test				pre-test				Diferencias		% diferenc (pre y post)	al 100%=90 encuestados
P R E G U N T A	**SI**	**NO**	**N/A**	**N/R**	**SI**	**NO**	**N/A**	**N/R**	**si**	**no**		
D. **CONTROLES DE ACCESO A DATOS Y PROGRAMAS:**												
D.1 Protección de las redes y comunicaciones												
Existe interconexión entre locales?	90				74				16		21.62	0.00
Cuenta con:												
- Acceso a internet (ancho de banda)	90				68				22		32.35	0.00
- Firewall o cortafuego físico	90				68				22		32.35	0.00
- Firewall Lógico		0		0		0		0				
- Servidor de dominio	90				22	68		68	68	-68	309.09	0.00
- Servidor proxy	90				68				22	0	32.35	0.00
- Switch core	90				68				22	0	32.35	0.00
- Switches de borde	90				68				22	0	32.35	0.00
- Switch de contingencia?	90				46	44		44	44	-44	95.65	0.00
Los switches están instalados e gabinetes ventilados?	90				68				22		32.35	0.00
Las canaletas están en buen estado?	90				68				22		32.35	0.00
El cableado de la red de datos está certificado? CAT:	84	0		0	34	56		56	50	-56	147.06	6.67
D.2 Protección de gestión de usuarios												
Los usuarios fueron informados por escrito sobre las buenas prácticas de seguridad para la selección y uso de sus contraseñas?	87				58				29		50.00	3.33
Las sesiones de los usuarios se desactivan tras un periodo definido de inactividad?	82				57				25		43.86	8.89
D.3 Mecanismos de identificación y autenticación									0			

El acceso al sistema es controlado con contraseña?	90				76				14		18.42	0.00
Están limitados los reintentos de acceso al sistema?	90				76				14		18.42	0.00
Se controla la existencia de datos faltantes?	87	0		0	44	46		46	43	-46	97.73	3.33
Los procedimientos están estandarizados?	87				44	46		B	43	-46	97.73	3.33
Se documenta el mantenimiento del sistema?	89				68				21		30.88	1.11
Los reportes impresos o la información mostrada en pantalla, identifican al usuario que envió el reporte?	83	5		5	21	69		69	62	-64	295.24	7.78
Los reportes cuidan la correlación de los documentos emitidos?	89				72				17		23.61	1.11
Reciben los niveles gerenciales reportes para la toma de decisiones?	89				72				17		23.61	1.11
D.4 Gestión de derechos de acceso												
La entidad adoptó una política de acceso a los sistemas, servicios informáticos y otros usos de la red?	89				48				41		85.42	1.11
Existen procedimientos para controlar la asignación de los derechos de acceso a los sistemas y demás servicios informáticos?	89				44	56		56	45	-56	102.27	1.11
Está controlado el uso y asignación de privilegios para el acceso?	89				48				41		85.42	1.11
Mantiene un registro de todos los privilegios asignados?	89				48				41		85.42	1.11
Se controla por escrito la asignación de contraseñas?	89				46				43		93.48	1.11
- Está restringido el acceso al software de seguridad?	89				48				41		85.42	1.11
- Está restringido el acceso a los programas fuente?	89				48				41		85.42	1.11
- Está restringido el acceso a la base de datos?	89				48				41		85.42	1.11
- Está restringido el acceso a las copias de respaldo?	89				48				41		85.42	1.11
- Se realizan controles periódicos para asegurar que no se hayan presentado cambios no autorizados en los programas?	83	5		5	43	47		47	40	-42	93.02	7.78
- Se han definido procedimientos de auditoría a la base de datos?	89				43	47		47	46	-47	106.98	1.11
- Se utiliza filtros de correo electrónico para bloquear los mensajes?	87				48				39		81.25	3.33
- Se utiliza filtros web para controlar el acceso a internet solo a páginas autorizadas?	89				48				41		85.42	1.11
E. **CONTINUIDAD DE NEGOCIO (Servicios de TI)**												
E.1 Copias de seguridad												

La entidad cuenta con procedimientos, aprobados, para la generación y resguardo de copias de respaldo?	90				37				53		143.24	0.00
Los medios magnéticos con copias de respaldo son almacenados en lugares seguros?	90				37				53		143.24	0.00
E.2 Planes de continuidad												
La Oficina de Informática cuenta con:												
- Normas internas sobre seguridad de la información en aplicación de la NTP ISO-IEC 17799-2007?	89				43	47		47	46	-47	106.98	1.11
- Plan de Contingencias Informático?	89				43	47		47	46	-47	106.98	1.11
- Pruebas periódicas del Plan de Contingencias Informático?	85	5		5	43	47		47	42	-42	97.67	5.56
- Centros alternativos de procesamiento de datos	87	3		3	43	47		47	44	-44	102.33	3.33

Nota. *Elaboración propia*

Tabla 27

Prueba de Kolmogorov-Smirnov para la muestra

		H3DIFERENCIAS
N		50
Parámetros normales[a,b]	Media	48,1200
	Desv. Desviación	24,74081
Máximas diferencias extremas	Absoluto	,218
	Positivo	,218
	Negativo	-,155
Estadístico de prueba		,218
Sig. asintótica(bilateral)		,000[c]

Nota. a = La distribución de prueba es normal. b = Se calcula a partir de datos. C. Corrección de significación de Lilliefors. 1=Lilliefors corregida.

Figura 12

Resumen de prueba de hipótesis

	Hipótesis nula	Prueba	Sig.	Decisión
1	Las categorías de H2ANTES se producen con probabilidades iguales.	Prueba de chi-cuadrado para una muestra	,556[1]	Retener la hipótesis nula.
2	La distribución de H2DESPUES es normal con la media 86,90 y la desviación estándar 6,320.	Prueba de Kolmogorov-Smirnov para una muestra	,000[1]	Rechazar la hipótesis nula.
3	La distribución de H2DIFERENCIAS es normal con la media 40,57 y la desviación estándar 23,842.	Prueba de Kolmogorov-Smirnov para una muestra	,010[1]	Rechazar la hipótesis nula.
4	La distribución de H3DESPUES es normal con la media 90,00 y la desviación estándar 0,000.	Prueba de Kolmogorov-Smirnov para una muestra	.	No se puede calcular.
5	La distribución de H3ANTES es normal con la media 52,35 y la desviación estándar 14,384.	Prueba de Kolmogorov-Smirnov para una muestra	,000[1]	Rechazar la hipótesis nula.
6	La distribución de H3DIFERENCIAS es normal con la media 48,12 y la desviación estándar 24,741.	Prueba de Kolmogorov-Smirnov para una muestra	,000[1]	Rechazar la hipótesis nula.

Nota. Se muestran significaciones asintóticas. El nivel de significación es de ,005

De la tabla 25, que los resultados indican que se ha incrementado en un alto porcentaje. La tabla 26 contiene los detalles del procesamiento de datos relacionados con la seguridad informática, donde se refleja que hubo en estas actividades, con la adquisición, uso y mantenimiento de los recursos de TI, tal como lo demuestra las cifras de la figura 12; por lo que se puede decir que se acepta la Hipótesis del investigador, y se demuestra que se han alcanzado los objetivos y metas del control interno.

V. DISCUSIÓN DE RESULTADOS

Con la metodología implementada se ha generado satisfacción en los usuarios y mejora en los resultados, todos los ítems considerados en el instrumento de medición han dado resultados positivos, llegando en algunos casos a tener una mejora del 100%.

En relación con lo que se venía haciendo y con lo que se hace después de la implementación ha mejorado en algunos actividades doce (12) veces más, en otros ha superado en veintidós (22) veces más las actividades que se habían realizado antes de implementar la metodología. Por lo que se puede deducir que la mejora ha sido sustancial después de implementación de la metodología, y encontrando una satisfacción en los encuestados.

Con la mejora en las actividades, se ha incrementado el uso de los recursos públicos para el bienestar de la sociedad, y también se tiene un control interno más eficaz y ágil en la evaluación de los datos registrados y evaluados en las oficinas o centros informáticos.

VI. CONCLUSIONES

6.1. Se ha mejorado el uso de infraestructura de las oficinas de TI, debido a que en algunas dependencias se han implementado equipos para alcanzar objetivos y metas trazadas con la ejecución de presupuesto anual.

6.2. Se optimizaron los procesos de adquisición, uso y mantenimiento de los recursos de TI. Mediante procedimientos adecuados, previa evaluación de las necesidades.

6.3. Se ha determinado normas de seguridad informática para el software y hardware en coordinación con los encargados de las oficinas de tecnologías de información.

6.4. Los recursos presupuestales que se invierten en mejorar las infraestructuras de las oficinas de tecnologías de información, con la finalidad de hacer más eficiente el control interno son directamente proporcionales a la cantidad y buen uso de estos; sin embargo, no están incluidos formalmente en los presupuestos anuales como meta, lo que no hace efectiva su implementación.

6.5. Es necesario apoyar e incentivar la integridad del funcionario pública e impulsar reformas anticorrupción en las diferentes instituciones del estado para optimizar el servicio que se le brinda a la sociedad.

VII. RECOMENDACIONES

7.1. Difundir la metodología propuesta en este trabajo de investigación para que mediante la capacitación, supervisión y control permanente al personal involucrado en la ejecución de las actividades se empiece a reducir las deficiencias y a optimizar el uso del gasto público presupuestado.

7.2. Que los titulares de las entidades implementen las políticas de modernización para implementar la administración por procesos; de tal manera que se mejore la infraestructura de las oficinas de TI, para una mejor ejecución del presupuesto, control interno y auditoría.

7.3. Que los titulares de las entidades difundan las normas, capaciten y sensibilicen a los colaboradores comprometidos con la ejecución del gasto público para mejorar los procesos, supervisión y control, a fin de conseguir los objetivos institucionales.

7.4. Que los órganos de control institucional de las entidades del sector público, cumplan con objetividad y transparencia la actividad relacionada a la evaluación del grado de madurez en la implementación del Sistema de Control Interno, generando indicadores para que en su momento nos permitan evaluar la efectividad de su funcionamiento.

7.5. Mantener la evaluación constante de los resultados generados después de la implementación de la metodología propuesta, para retroalimentar al sistema y propender a la mejora continua.

VIII. REFERENCIAS

Auditoría en Sistemas de Información. (4 de mayo de 2012). Monografías. https://www.monografias.com/trabajos16/auditoria-de-informacion/auditoria-de-informacion

Castello, R. (1998). *Auditoría en Entornos Informáticos*. Editorial Universidad Nacional de Córdoba.

Constitución Política del Perú [Const.] Art. 82, 29 de diciembre de 1993. https://cdn.www.gob.pe/uploads/document/file/198518/Constitucion_Politica_del_Peru_1993.pdf?v=1594239946

Decreto Supremo N° 004-2013-PCM, Política Nacional de Modernización de la Gestión Pública al 2021. (9 de enero de 2013). Presidencia del Consejo de Ministros del Perú. Numeral 1.2 del anexo. https://cdn.www.gob.pe/uploads/document/file/357174/DS-004-2013-PCM-Aprueba-la-PNMGP.pdf?v=1567454992

Hirsch, A. (2013). *La Ética Profesional Basada en Principios y su Relación con la Docencia.* Instituto de Investigaciones sobre la Universidad y la Educación. Universidad Nacional Autónoma de México

Ley Nº 27785 – Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República. (23 de julio de 2002). Congreso de la República del Perú. Capítulo II. https://leyes.congreso.gob.pe/Documentos/Leyes/27785.pdf

Ley N° 28716 – Ley de Control Interno de las Entidades del Estado. (18 de abril de 2006). Congreso de la República del Perú. Título III. https://www.leyes.congreso.gob.pe/Documentos/Leyes/28716.pdf

Oficina Superior de Contrataciones del Estado. [OSCE]. (22 de junio de 2009). *Planeamiento/Organización.* *https://www.transparencia.gob.pe/enlaces/pte_transparencia_enlaces.aspx?id_entidad=10&id_tema=5&ver=D#.Y53sf33MLIU*

Perú Contable. (22 de abril de 2021). *Listado de Ministerios, Regiones y Municipalidades*. https://www.perucontable.com/listado-de-ministerios-regiones-municipalidades/

Portal de Transparencia Estándar. (19 de febrero de 2009). *Organismos Autónomos.* *https://www.transparencia.gob.pe/buscador/pte_transparencia_listado_entidades_poder.aspx?Tipo_Pod=4*

Quevedo, D. y Ramírez E. (2006). *Análisis comparativo entre los enfoques modernos de Control Interno: COSO, COCO y MICIL.* Universidad de Carabobo.

Resolución de Contraloría N° 320-2006-CG. Normas de Control Interno. (2006, 3 de noviembre). Contraloría General de la República del Perú. Artículo primero. https://doc.contraloria.gob.pe/libros/2/pdf/RC_320_2006_CG.pdf

Resolución Ministerial N° 246-2007-PCM. Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnologías de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2da. Edición. En todas las entidades integrantes del Sistema Nacional de Informática. (2007, 26 de agosto). Presidencia del Consejo de Ministros del Perú. Artículo primero. https://cdn.www.gob.pe/uploads/document/file/357317/RM_246-2007-PCM.pdf?v=1567466237

Resolución de Contraloría N°273-2014-CG. Normas Generales de Control Gubernamental, y su modificatoria. (2014, 12 de mayo). Contraloría General de la República del Perú. Artículo primero. https://doc.contraloria.gob.pe/libros/2/pdf/RC_273_2014_CG.pdf

Resolución de Contraloría N° 458-2008-CG. Guía para la Implementación del Sistema de Control Interno de las entidades del Estado. (30 de octubre de 2008). Contraloría General de la República del Perú. Artículo primero. https://cdn.www.gob.pe/uploads/document/file/5498/RCG458-2008-CG.pdf?v=1529770756

Auditoría. (28 de noviembre de 2007). Rincón del Vago. https://html.rincondelvago.com/auditoria_7.html

Rivas, G. (1988). *Auditoría Informática.* Ediciones Díaz de Santos.

Rivero A, y Campos, L. (2005). *Antecedentes y evolución del Control Interno. Su desarrollo en Cuba.* https://www.monografias.com/trabajos59/evolucion-control-interno/evolucion-control-interno

Servicio de Administración Tributaria. [SAT]. (22 de junio de 2009). *Planeamiento/Organización. https://www.sat.gob.pe/transparenciav3/Transparencia*

Sindicatura General de la Nación [SIGEN]. (23 de noviembre de 2018). *Unidades de Auditoría Interna*. https://www.argentina.gob.ar/sigen/unidades-de-auditoria-interna

A N E X O S

ANEXO A

CARTA DE PRESENTACIÓN

Lima, 02 de Julio 2018

Señor:

Dra. Ingº. Mónica Juanita Romero valencia

Presente

Asunto: **SOLICITO VALIDACIÓN DE INSTRUMENTOS A TRAVÉS DE JUICIO DE EXPERTO.**

Es muy grato comunicarme con usted para expresarle mi saludo y así mismo, hacer de su conocimiento que siendo estudiante de la Escuela Universitaria de Postgrado en Ingeniería de Sistemas de la UNFV, Promoción -2009, requiero validar los instrumentos con los cuales recogeré la información necesaria para poder desarrollar mi investigación y con la cual optaré el grado de Maestra en Ingeniería de Sistemas.

El título de mi proyecto de investigación es**: "**METODOLOGIA PARA AUDITAR LA GESTION INFORMÁTICA EN ENTIDADES SUJETAS AL SISTEMA NACIONAL DE CONTROL, COMO IMPLEMENTACIÓN DEL SISTEMA DE CONTROL INTERNO DE LAS ENTIDADES "**,** y siendo imprescindible contar con la aprobación de docentes especializados para poder aplicar los instrumentos en mención, he considerado conveniente recurrir a usted, ante su connotada experiencia en temas de investigación educativa.

El expediente de validación, que le hago llegar contiene:

Anexo N° 1: Carta de presentación

Anexo N° 2: Operacionalización de las variables

Anexo N° 3: Certificado de validez de contenido de los instrumentos

Anexo Nº 4: Matriz de consistencia.

Expresándole mi sentimiento de respeto y consideración me despido de usted, no sin antes agradecerle por la atención que dispense a la presente.

Atentamente.

_____

ARTURO ENRIQUE BONIFAZ OCAMPO

D.N.I: 33408727

Reg. CIP Nº 31953

ANEXO B

VALIDACIÓN DE INSTRUMENTO DE ENCUESTA

PARA INSTITUCIONES COMPROMETIDAS EN GESTION DE AUDITORIA INFORMATICA

ENCUESTA DE OPINIÓN EN LA INSTITUCION:…….

CONDICION DEL ENCUESTADO……

Consideraciones para responder:

5	4	3	2	1
Siempre	Casi siempre	A veces	Casi nunca	Nunca

5	4	3	2	1
Totalmente de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo

***Nota*:** Colocar un solo un número en cada casillero de la pregunta que Usted considere adecuado como satisfacción de repuesta a la interrogante leída**:**

1. ¿Toma mucho tiempo en obtener la información necesaria del sistema para la toma de decisiones?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

2. ¿Cree usted que la aplicación de una buena práctica para el proceso de requerimiento de información contribuya a mejorar la gestión de auditoria informática?

a) Totalme ☐ b) De acuerdo ☐ c) Indeciso ☐ d) En desacuerd ☐ e) Totalmente ☐

de acuerdo en desacuerdo

3. ¿Cree usted que la aplicación de una buena práctica para el proceso de requerimiento información contribuya a mejorar el control y seguimiento del uso de fondos del presupuesto público nacional?

a) Totalme ☐ b) De acuerdo ☐ c) Indeciso ☐ d) En desacuerdo ☐ e) Totalmente ☐

de acuerdo en desacuerdo

4. ¿Cree usted que la aplicación de una buena práctica para el proceso de requerimiento de información permita que todo el personal de ejecución del presupuesto público trabaje bajo un procedimiento definido y estandarizado?

a) Totalme ☐ b) De acuerdo ☐ c) Indeciso ☐ d) En desacuerdo ☐ e) Totalmente ☐

de acuerdo en desacuerdo

5. ¿La herramienta y/o formato que utiliza para el requerimiento de información es de ayuda

para realizar los respectivos informes previos o finales de auditoria?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

6. La gestión y servicios que brinda la entidad pública a la que pertenece, satisface a los usuarios con lo previsto en el presupuesto público anual ¿Cree que es el adecuado?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

7. ¿Considera que se está manejando correctamente los fondos públicos con el uso de la nueva metodología de gestión de auditoria informática?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

8. ¿Considera correcta la herramienta y/o formato utilizado para hacer los pasos de cada escenario en los casos de evaluación para informes de auditoría parcial y/o final?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

9. ¿Cree usted que la aplicación de la nueva metodología ha contribuido en disminuir la cantidad de incidencias en el proceso del control y auditoria del gasto público?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

10. ¿Se llegan a terminar a tiempo, todos los requerimientos de información para los informes previos ó finales de auditoria?

a) siempre ☐ b) casi siempr ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

11. ¿El personal que labora en el área de auditoria informática está capacitado para dar un buen servicio?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

12. ¿En sus informes parciales y/o finales contempla las buenas prácticas?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

13. ¿Cree usted que los informes que maneja tiene los datos adecuados y reales para los análisis pertinentes?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

14. ¿Cree usted que su equipo de trabajo necesita capacitaciones en nuevas prácticas y metodología que se utiliza en la actualidad?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

15. ¿Cuándo se reúne con la Jefatura Institucional para ver los temas de auditoria, siempre llegan acuerdos por si encuentran incidencias?

a) Siempre ☐ b) Casi siempre ☐ c) A veces ☐ d) Casi nunca ☐ e) Nunca ☐

16¿Cuándo ha realizado pruebas funcionales del sistema informático en base al requerimiento realizado han tenido muchos errores?

a)Siempre ☐ b)Casi siempre ☐ c)A veces ☐ d)Casi nunca ☐ e)Nunca ☐

17¿Cree usted que las observaciones que encuentra en los documentos y/o pruebas se genere en base al formato de requerimientos?

a)Siempre ☐ b)Casi siempre ☐ c)A veces ☐ d)Casi nunca ☐ e)Nunca ☐

18¿Considera adecuada y oportuna la orientación que le brinda el cliente durante una explicación del requerimiento?

a)Siempre ☐ b)Casi siempre ☐ c)A veces ☐ d)Casi nunca ☐ e)Nunca ☐

19¿Considera adecuado el equipamiento tecnológico que presenta el proyecto (computadoras, impresoras, etc.), para atender al usuario?

a)Siempre ☐ b)Casi siempre ☐ c)A veces ☐ d)Casi nunca ☐ e)Nunca ☐

20¿Se llegan a terminar a tiempo, todos los requerimientos del cliente?

a)Siempre ☐ b)Casi siempr ☐ c)A veces ☐ d)Casi nunca ☐ e)Nunca ☐

"Gracias por su participación en la mejora de gestión institucional"

ANEXO C

EVALUACION DE LOS CONTROLES GENERALES DE TECNOLOGIAS DE LA INFORMACIÓN - CGTI

(SE REFIERE A LA SITUACIÓN ACTUAL DEL SERVICIO INFORMÁTICO)

OBJETIVO:
Tomar conocimiento sobre los controles generales de tecnologías de la información - CGTI, en relación a las actividades realizadas por la Oficina de TI de la entidad y teniendo en cuenta las cinco categorías en las que se agrupan los CGTI y sus respectivas sub categorías. En aplicación a lo indicado en el Manual de Auditoría Financiera Gubernamental (MAFGU), aprobado por Resolución de Contraloría Nº 445-2014-CG, de fecha 03 de octubre de 2014.

DEL DIRECTOR DE LA OFICINA DE TI:

Apellidos y nombres: _____ **DNI:** _____

Situación contractual: _____ **Desde:** _____

Siglas: N/A: No aplica REF.P/T: Para indicar un documento adjunto ET=En trámite
Nivel del riesgo: mi= mínimo, B=Bajo, M=Moderado, A=Alto

P R E G U N T A	REF P/T	CONTROLADO			NIVEL DEL RIESGO
		SI	NO	N/A	
A. MARCO ORGANIZATIVO:					
A.1 Organización y personal de TI					
La Oficina de Informática realiza las siguientes funciones:					
- Elabora políticas planes, normas y procedimientos de TICs?					
- Análisis, desarrollo y mantenimiento de sistemas?					
- Control de Calidad de los sistemas?					
- Soporte Técnico a los usuarios?					
- Seguridad Informática?					
- Estas funciones están definidas en el ROF?					
- El MOF describe las funciones de todo el personal considerado en el CAP?					
- La gerencia asignó, por escrito, funciones al personal cuyo cargo no está considerado en el MOF?					
Se ha nombrado al Oficial de Seguridad de la Información?					
A.2 Planificación, políticas y procedimientos					
La Oficina de Informática cuenta con los siguientes documentos de gestión:					
- Plan Estratégico de Tecnologías de la Información?					
- Plan Estratégico de Gobierno Electrónico o similar?					
- Plan Operativo Informático aprobado y remitido a la ONGEI-PCM?					
- Evaluación del POI aprobado y remitido a la ONGEI-PCM?					
- Políticas y normas de gestión de la seguridad de la información?					
- Planes de formación y concientización en seguridad de TI?					
- Plan o cronograma de mantenimiento preventivo de los equipos de cómputo?					
- Procedimientos de gestión de riesgos de TI?					
- Directivas para la gestión de las bases de datos de los sistemas que soportan los procesos administrativos.					
- Normas internas sobre uso de internet y correo electrónico?					
B. **GESTIÓN DE CAMBIOS EN SISTEMAS:**					
B.1 Adquisición de sistemas					

PREGUNTA	REF P/T	CONTROLADO			NIVEL DEL RIESGO
		SI	NO	N/A	
La entidad adquirió algún sistema para el manejo financiero y presupuestal con el presupuesto del ejercicio auditado?					
La entidad adquirió otro tipo de software con el presupuesto del ejercicio auditado?					
Elaboró el Informe Técnico Previo de Evaluación de Software antes de adquirir los programas antes mencionados?					
B.2 Desarrollo y mantenimiento de sistemas					
Metodología de desarrollo de software:					
- Existe?					
- Se aplica?					
- Es suficiente?					
El desarrollo o mantenimiento del software requiere:					
- Autorización del Jefe del Usuario?					
- Aprobación del Jefe de la OI?					
- Aprobación de procedimientos de prueba de parte del usuario?					
- Aprobación final del usuario antes de la puesta en marcha?					
- Entornos físicos independientes para el desarrollo, pruebas y producción de software?					
B.3 Gestión de cambios en los sistemas					
La entidad cuenta con software administrador de cambios o de versiones?					
Se documenta el mantenimiento de los sistemas, desde la solicitud hasta la aceptación final por parte del usuario?					
Se generan o actualizan los manuales respectivos?					
C. **OPERACIONES DE LOS SISTEMAS DE INFORMACIÓN:**					
C.1 Operaciones TI					
La entidad cuenta con inventario de hardware actualizado?					
La entidad cuenta con inventario de software actualizado?					
Lleva una bitácora sobre las fallas y mantenimientos realizados a los equipos informáticos?					
Existe software instalado en la entidad que no cuenta con licencias o autorizaciones de uso?					
Se utiliza algún programa para detectar en la red la instalación de software ilegal o no autorizado?					
Se encuentran protegidos con software antivirus legal y actualizado:					
• Los servidores?					
• Las estaciones de trabajo?					
Se monitorea desde La Oficina de Informática las actualizaciones del antivirus?					
C.2 Seguridad física					
Controles de acceso físico a la entidad					
- El local de la entidad está protegido contra robos?					
- Se controla el ingreso de extraños al local?					
- Existe un circuito cerrado de video vigilancia del local?					
Controles de acceso físico al centro de procesamiento de datos					
- El ambiente está diferenciado del resto de la infraestructura?					
- Cuenta con un ambiente previo (zona de acceso y control)?					
- Se accede mediante control biométrico?					
- Se registra a las personas que acceden a la sala de servidores?					
- Posee piso técnico o techo con placas suspendidas?					
- Los gabinetes están dispuestos de manera adecuada?					
- Los servidores están instalados dentro de sus racks respectivos?					
- Existen servidores compatibles?					
- Existen otros elementos no propios de una sala de servidores?					
- Se han instalado cámaras de video o detectores de intrusos?					
- Los equipos están conectadas a UPSs?.					
- Los equipos están conectadas a circuitos con puesta a tierra?.					
- Esta canalizada la transferencia de frio o calor?					

PREGUNTA	REF P/T	CONTROLADO			NIVEL DEL RIESGO
		SI	NO	N/A	
- El ambiente cuenta con:					
o Sistema contra incendios					
o Detectores de inundación					
o Detectores de humo					
C.3 Servicios contratados a terceros					
Los requerimientos de servicios de servicio de TI obedecen a una programación?					
La Oficina de Informática controla el cumplimiento de los servicios contratados?					
D. **CONTROLES DE ACCESO A DATOS Y PROGRAMAS:**					
D.1 Protección de las redes y comunicaciones					
Existe interconexión entre locales?					
Cuenta con:					
- Acceso a internet (ancho de banda)					
- Firewall o cortafuego físico					
- Firewall Lógico					
- Servidor de dominio					
- Servidor proxy					
- Switch core					
- Switches de borde					
- Switch de contingencia?					
Los switches están instalados e gabinetes ventilados?					
Las canaletas están en buen estado?					
El cableado de la red de datos está certificado? CAT:					
D.2 Protección de gestión de usuarios					
Los usuarios fueron informados por escrito sobre las buenas prácticas de seguridad para la selección y uso de sus contraseñas?					
Las sesiones de los usuarios se desactivan tras un periodo definido de inactividad?					
D.3 Mecanismos de identificación y autenticación					
El acceso al sistema es controlado con contraseña?					
Están limitados los reintentos de acceso al sistema?					
Se controla la existencia de datos faltantes?					
Los procedimientos están estandarizados?					
Se documenta el mantenimiento del sistema?					
Los reportes impresos o la información mostrada en pantalla, identifican al usuario que envió el reporte?					
Los reportes cuidan la correlación de los documentos emitidos?					
Reciben los niveles gerenciales reportes para la toma de decisiones?					
D.4 Gestión de derechos de acceso					
La entidad adoptó una política de acceso a los sistemas, servicios informáticos y otros usos de la red?					
Existen procedimientos para controlar la asignación de los derechos de acceso a los sistemas y demás servicios informáticos?					
Está controlado el uso y asignación de privilegios para el acceso?					
Mantiene un registro de todos los privilegios asignados?					
Se controla por escrito la asignación de contraseñas?					
- Está restringido el acceso al software de seguridad?					
- Está restringido el acceso a los programas fuente?					
- Está restringido el acceso a la base de datos?					
- Está restringido el acceso a las copias de respaldo?					
- Se realizan controles periódicos para asegurar que no se hayan presentado cambios no autorizados en los programas?					
- Se han definido procedimientos de auditoría a la base de datos?					
- Se utiliza filtros de correo electrónico para bloquear los mensajes?					
- Se utiliza filtros web para controlar el acceso a internet solo a páginas autorizadas?					

P R E G U N T A	REF P/T	CONTROLADO			NIVEL DEL RIESGO
		SI	NO	N/A	
E. **CONTINUIDAD DE NEGOCIO (Servicios de TI)**					
E.1 Copias de seguridad					
La entidad cuenta con procedimientos, aprobados, para la generación y resguardo de copias de respaldo?					
Los medios magnéticos con copias de respaldo son almacenados en lugares seguros?					
E.2 Planes de continuidad					
La Oficina de Informática cuenta con:					
- Normas internas sobre seguridad de la información en aplicación de la NTP ISO-IEC 17799-2007?					
- Plan de Contingencias Informático?					
- Pruebas periódicas del Plan de Contingencias Informático?					
- Centros alternativos de procesamiento de datos					

Fuente:

Dirección de Oficina de TI

ANEXO D

MATRIZ DE EVALUACION DE LOS RIESGOS INHERENTES A LA OFICINA DE TI

ANEXO D

Matriz de Evaluacion de los Riesgos inherentes a la Oficina de TI

Proceso: **Dueño del Proceso:**

Objetivo: **Evaluador:** **Fecha de Evaluación:**

Item Nº	I. Riesgos						II. Controles					III. Respuesta al Riesgo		IV. Planes de Acción				V. Seguimiento	
	Descripción de Riesgo	Causa del Riesgo	Tipo de Riesgo	Evaluación Riesgo Inherente			Actividad	Responsable	Documento	Status de implementación (No impl. En proceso	Tipo		Evaluación de Riesgo Controlado			Tratamiento (Evadir Aceptar Enfrentar)	Justificación	Descripción	Responsable	Fecha de implementación	Comentario	Status	Comentario
				Impacto	Probabilidad	Nivel Inherente					Preventivo / Detectivo	Manual / Automatizado	Impacto	Probabilidad	Nivel Residual								
			Estratégico	2 - MODERAD	2 - POSIBLE	R.MODERADO					PREVENTIVO	MANUAL	1 - LEVE	2 - POSIBLE	R.TOLERABLE								
			Tecnologico	3 - DESASTRO	2 - POSIBLE	R.IMPORTANTE					DETECTIVO	AUTOMATIZADO	2 - MODERADO	2 - POSIBLE	R.MODERADO								
			Financiero	2 - MODERAD	1 - IMPROBABLE	R.TOLERABLE					PREVENTIVO	MANUAL	3 - DESASTROSO	3 - PROBABLE	R.IMPORTANTE								
			De cumplimie	1 - LEVE	3 - PROBABLE	R.MODERADO					DETECTIVO	AUTOMATIZADO	3 - DESASTROSO	2 - POSIBLE	R.IMPORTANTE								
			Operativo	2 - MODERAD	3 - PROBABLE	R.IMPORTANTE					DETECTIVO	AUTOMATIZADO	2 - MODERADO	2 - POSIBLE	R.MODERADO								
			Operativo	2 - MODERAD	1 - IMPROBABLE	R.TOLERABLE					PREVENTIVO	AUTOMATIZADO	2 - MODERADO	1 - IMPROBABLE	R.TOLERABLE								

Actividades y procedimientos frecuentes:

SOPORTE TÉCNICO

Reporte de incidencias y solicitudes

Registro de incidencias y solicitudes

Atención de incidencias y solicitudes

Supervisión de incidencias y solicitudes

ADMINISTRAR RESPALDO DE INFORMACIÓN DIARIA Y MENSUAL

Respaldo diario

Respaldo mensual

Respaldo a demanda

Prueba de cintas

Supervisión de cintas y respaldos de información

ADMINISTRACIÓN DE OPERACIONES

Creación de cuentas de correo empresarial

Entrega de credenciales del correo electrónico empresarial

Bloqueo de cuentas de correo electrónico empresarial

Eliminación de cuenta de correo electrónico empresarial

Soporte técnico al servicio de correo electrónico empresarial

Administrar accesos a servicios controlados por el firewall

Supervisar estado del antivirus

ADMINISTRACIÓN DE SERVIDORES Y REDES

Sobre los servidores de red

Sobre administración de equipos de red

Del mantenimiento de servidores y equipos de red

ADMINISTRACIÓN DE RED ELÉCTRICA

Ejecución del mantenimiento preventivo de UPS

Ejecución del mantenimiento preventivo de grupo electrógeno

SEGURIDAD FÍSICA DEL DATA CENTER TIC

Ingreso del personal autorizado a la sala de servidores

Ingreso de visitantes a la sala de servidores

Analisis de ingresos

Mantenimiento de los accesos a la sala de servidores}

ANEXO E

MATRIZ DE CONSISTENCIA

TÍTULO: "METODOLOGÍA PARA AUDITAR LA GESTION INFORMÁTICA EN ENTIDADES PUBLICAS SUJETAS AL SISTEMA NACIONAL DE CONTROL"							
	PROBLEMA	**OBJETIVO**	**HIPÓTESIS**	**VARIABLES**	**INDICADORES**	**MÉTODOS**	**TÉCNICAS E INSTRUMENTOS**
PRINCIPAL O GENERAL	¿Es posible emitir una opinión acertada sobre el estado del sistema informático en una entidad del sector público sin contar con una metodología adecuada?	Diseñar una metodología para auditar y emitir una opinión sobre la implementación del sistema informático en las entidades públicas sujetas al Sistema Nacional de Control.	Una metodología adecuada para auditar la gestión informática en las entidades públicas; mejorará el control interno y uso de los recursos, permitiendo emitir un dictamen oportuno, acertado y sustentado	**Variable Independiente (X):** Metodología para auditar la gestión informática. **Variable Dependiente (Y):** - Mejorar el control interno. - Eficacia en el uso de los recursos. - Emitir opinión oportuna.	- Acciones orientadas a la capacitación. - Acciones orientadas a la gestión interna. - Obsolescencia del hardware. - Mantenimiento del hardware. - Eficacia en el cumplimiento de actividades. - Eficiencia en el uso del presupuesto. - Eficacia en el uso del hardware - Eficacia en el desarrollo y/o uso del software. - Evidencia competente. - Evidencia relevante. - Evidencia suficiente. - Evidencia oportuna. - Tiempos en la	**Tipo de Estudio** Aplicada Explicativa Retrospectiva Retro electiva Transversal Comparativa **Diseño** Experimental de tipo Experimental puro	**Técnicas** - Entrevista individual - Cuestionarios **Instrumentos** - Formato de entrevistas - Grabaciones - Balotario de preguntas - Fichas. - Cuadros sinópticos. - Fotocopias. - Diagramas. - Computador. - DVD´s, USB - Redes sociales - Estadística inferencial

SECUNDARIOS O ESPECÍFICOS	**PROBLEMAS**	**OBJETIVOS**	**HIPÓTESIS**	**VARIABLES**	entrega de informes preliminares y finales. - Presupuesto institucional destinado a TI. - Incremento porcentual del gasto público. - Cantidad de proyectos desarrollados con la implementación		
	¿La organización e infraestructura de las oficinas de TI contribuye en la consecución de los objetivos y metas?	Optimizar el uso de la infraestructura de las oficinas de TI en relación con las metas del Plan Estratégico	La mejora de la organización e infraestructura de las oficinas de TI incide en la gestión, objetivos y metas.	- Organización e infraestructura de la oficina de TI. - Gestión, objetivos y metas.			
	¿Las adquisiciones, uso y mantenimiento de los recursos de TI inciden en la gestión de la entidad?	Determinar los procesos de adquisición, uso y mantenimiento de los recursos de TI	La gestión informática depende de la eficiencia en las adquisiciones, uso y mantenimiento de los recursos de TI en la entidad.	- Gestión informática. - eficiencia - Adquisición de Hw. y Sw. - Uso de Hw. y Sw. - Mnto de Hw. y Sw.			
	¿Los sistemas informáticos instalados en la entidad satisfacen a los usuarios?	Evaluar los sistemas informáticos instalados en la entidad	Los Sistemas informáticos instalados satisfacen las necesidades de los usuarios.	- Metodología para auditar la gestión informática. - Validación de procesos del Sw..			
	¿El hardware y software instalado cumple con las normas de Seguridad Informática?	Determinar normas de seguridad Informática para para el software y hardware.	La entidad que no adopta y actualiza sus normas de seguridad de TI puede tener caídas que afecten la gestión institucional	- Metodología para auditar la gestión informática. - Normas de seguridad en TI.			