DEFINICIÓN DE UNA METODOLOGÍA PARA LA ELABORACIÓN DE AUDITORÍAS DE SISTEMAS INFORMÁTICOS EN ENTIDADES DEL SISTEMA NACIONAL DE CONTROL PERUANO

José Carbajal-Romero

Lima, abril de 2013

FACULTAD DE INGENIERÍA

Master en Dirección Estratégica en Tecnologías de la Información

Carbajal, J. (2013). *Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano*. Tesis de Master en Dirección Estratégica en Tecnologías de la Información MDETI. Universidad de Piura. Facultad de Ingeniería. Lima, Perú.

UNIVERSIDAD DE PIURA
FACULTAD DE INGENIERIA

"Definición de una metodología para la elaboración de auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano"

Tesis para optar el Grado de Master en Dirección Estratégica en Tecnologías de la Información

Ing. José Alberto Carbajal Romero

Asesor: Ing. Omar Hurtado Jara

Piura, Abril 2013

A Dios, por darme el gran regalo de la vida.

A mis padres Rosa y Roque por su amor, esfuerzo y dedicación.

A mis abuelita Rosa, por ser siempre un ejemplo de vida a seguir.

A toda mi familia, por tratar siempre de ayudarme.

A mis profesores por sus valiosas enseñanzas.

Al Ing. Omar Hurtado Jara por su valioso apoyo.

Prólogo

En el Perú, la auditoría de sistemas informáticos es un tipo de auditoría relativamente nueva, que se viene aplicando en el sector público y privado. Al respecto, en el sector público peruano las auditorías (incluida las auditorías de sistemas informáticos) deben de realizarse en función del marco normativo aplicable a las entidades integrantes del Sistema Nacional de Control Peruano.

Al respecto, la normatividad peruana vigente no cuenta con una guía metodológica explícita de cómo realizar las auditorías de sistemas informáticos en el sector público peruano, debiendo indicar que en las entidades integrantes del Sistema Nacional de Control Peruano es requisito indispensable el cumplimiento del marco normativo peruano. Sin embargo, se debe cumplir y aplicar correctamente la normatividad emitida por la Contraloría General de la República, en su calidad de ente rector técnico del Sistema Nacional de Control Peruano.

Sobre el particular, es de resaltar la importancia de las auditorías de sistemas informáticos ya que contribuyen con recomendaciones (producto de los informes emitidos) a identificar situaciones que afectarían el cumplimiento de los objetivos institucionales de las entidades del sector público peruano; y es en ese sentido, que dichas entidades públicas pueden disponer las medidas correctivas que permitan corregir las situaciones identificadas por los auditores gubernamentales.

Resumen

El presente trabajo de tesis tiene como objetivo principal proponer una metodología que permita guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos que se realizan en el sector público peruano.

Para alcanzar dicho objetivo, se han planteado los siguientes objetivos específicos:

- Aplicar la normativa emitida por la Contraloría General de la República en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos.
- Aplicar la normativa emitida por otras entidades del Estado Peruano en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos.
- Aplicar los estándares internacionales en la elaboración de la propuesta metodológica relacionada a las auditorías de sistemas informáticos.

Al respecto, la presente guía metodológica se ha realizado en concordancia al marco normativo aplicable a las entidades del Sistema Nacional de Control Peruano utilizando en su elaboración los marcos de referencia de organismos internacionales. Dicha guía metodológica se convierte en una herramienta de consulta para las auditores gubernamentales que realizan auditorías en el sector público, contribuyendo de esta manera a realizar auditorías de una manera más eficiente y eficaz, facilitando la identificación de riesgos asociados a los controles de los procesos informáticos auditados así como optimizar el tiempo invertido en la realización de auditorías de tipo informático.

Índice General

Introducción

El presente trabajo de tesis plantea una metodología que permite guiar el proceso de auditorías de sistemas informáticos en el sector público peruano, el cual es realizado por los auditores gubernamentales del Sistema Nacional de Control Peruano.

Al respecto, la Contraloría General de la República en su calidad de ente técnico rector del Sistema Nacional de Control Peruano establece disposiciones necesarias para articular los procesos de control gubernamental de las diversas entidades del sector público con la finalidad que la gestión de los recursos, bienes y operaciones de las entidades públicas se efectúe correcta y eficientemente.

En ese sentido, el presente trabajo de tesis se ha estructurado de la siguiente manera:

- En el Capítulo 1 se detalla la normativa emitida por la Contraloría General de la República y otras entidades del Estado (ONGEI y normativa propia de cada entidad) así como marcos de referencia emitidos por diversas entidades internacionales (COSO, ISACA e ISO/IEC) que sirve como base para proponer una metodología que permite guiar el proceso de auditorías de sistemas informáticos en el sector público peruano.

- En el Capítulo 2 se detalla la metodología propuesta que permite guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en la realización de auditorías de sistemas informáticos en el sector público peruano, utilizando como base la normativa detallada en el Capítulo 1.

- En el Capítulo 3 se detalla la aplicación y validación de la metodología propuesta en un órgano de control institucional perteneciente al Sistema Nacional de Control Peruano, utilizando como base la metodología propuesta detallada en el Capítulo 2 del presente trabajo de tesis.

Capítulo 1

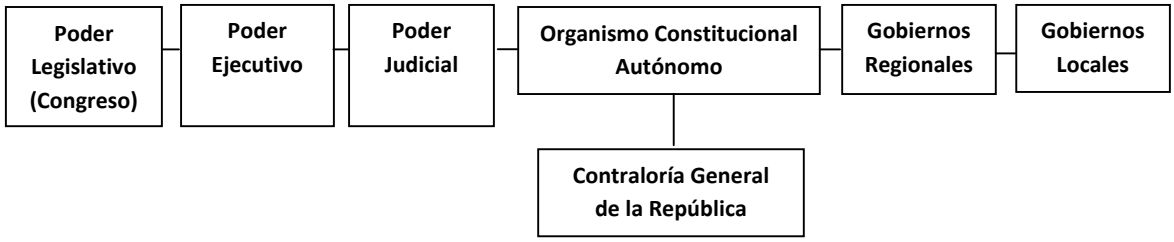
Marco normativo aplicable al proceso de auditorías de sistemas informáticos del Sistema Nacional de Control Peruano en el Sector Público Peruano.

Antes de proceder a detallar el marco normativo aplicable al proceso de auditorías de sistemas informáticos en el Sector Público Peruano es importante tener en cuenta que el Estado Peruano está conformado por el Poder Legislativo, Poder Ejecutivo, Poder Judicial, Organismos Constitucionales Autónomos, Gobiernos Regionales y Gobiernos Locales; los cuales a su vez están integrados por una serie de entidades que conforman el Sector Público Peruano.

Sobre el particular, el Poder Legislativo es el encargado de emitir, entre otros, las normas que regulan la labor del control gubernamental así como las relacionadas a temas informáticos. Dicho poder del Estado, a través del Congreso de la República, emitió la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República. Asimismo, la Constitución Política del Perú del año 1993 emitida por el Congreso Constituyente Democrático, estableció en su Artículo 82° que la Contraloría General de la República es una entidad descentralizada de Derecho Público que goza de autonomía conforme a su ley orgánica, siendo este organismo autónomo el órgano superior del Sistema Nacional de Control, encargándose de supervisar los actos de las instituciones sujetas a control gubernamental.

Del mismo modo, el Poder Ejecutivo se encarga de reglamentar las normas del Poder Legislativo vinculadas, entre otras, las relacionadas a las funciones de control gubernamental así como las relacionadas a temas informáticos. Asimismo, el Poder Judicial acoge, entre otros, las denuncias que se sustentan en los informes emitidos por el Sistema Nacional de Control Peruano para su respectiva investigación y pronunciamiento correspondiente, con el fin de determinar responsabilidad civil o penal. Además, son parte del Estado Peruano los gobiernos regionales y locales (provincias, distritos y centros poblados), tal como se muestra en el siguiente gráfico:

Gráfico N° 1.1. **Organización del Estado Peruano**



Estando a lo comentado en los párrafos precedentes, se procede a detallar el marco normativo aplicable a las auditorías de sistemas informáticos en el Sector Público Peruano:

1.1. Normativa relacionada al Sistema Nacional de Control Peruano y Contraloría General de la República

1.1.1. Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República

La Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República (Ley N° 27785) del 22.JUL.2002 establece las normas que regulan el ámbito, organización, atribuciones y funcionamiento del Sistema Nacional de Control y de la Contraloría General de la República con el objetivo de obtener un apropiado, oportuno y efectivo ejercicio del control gubernamental con la finalidad de contribuir al mejoramiento de las actividades y servicios de la entidad pública en beneficio del país, tal como se detalla a continuación:

1.1.1.1. Sistema Nacional de Control

Es el conjunto de órganos de control, normas, métodos y procedimientos, estructurados e integrados funcionalmente, destinados a conducir y desarrollar el ejercicio del control gubernamental. Comprende todas las actividades y acciones en los campos administrativo, presupuestal, operativo y financiero de las entidades y alcanza al personal que presta servicios en ellas, independientemente del régimen que las regule. El Sistema Nacional de Control está conformado de la siguiente manera:

a. Contraloría General de la República.
b. Todas las unidades orgánicas responsables de la función de control gubernamental (Órganos de Auditoría Interna o también llamados Órganos de Control Institucional).

c. Sociedades de auditoría externa independientes cuando sean designadas por la Contraloría General.

Gráfico N° 1.2. **Conformación del Sistema Nacional de Control**

1.1.1.2. Contraloría General de la República

Es el ente técnico rector del Sistema Nacional de Control con autonomía administrativa, funcional, económica y financiera; teniendo como misión, dirigir y supervisar con eficiencia y eficacia el control gubernamental. Entre las principales funciones de la Contraloría General se encuentran:

- Tener acceso en cualquier momento y sin limitación a los registros, documentos e información de las entidades, aun cuando sean secretos.
- Supervisar y garantizar el cumplimiento de las recomendaciones que se deriven de los informe de control emanados de cualquiera de los órganos del Sistema.
- Aprobar el Plan Nacional de Control y los planes anuales de control de las entidades.

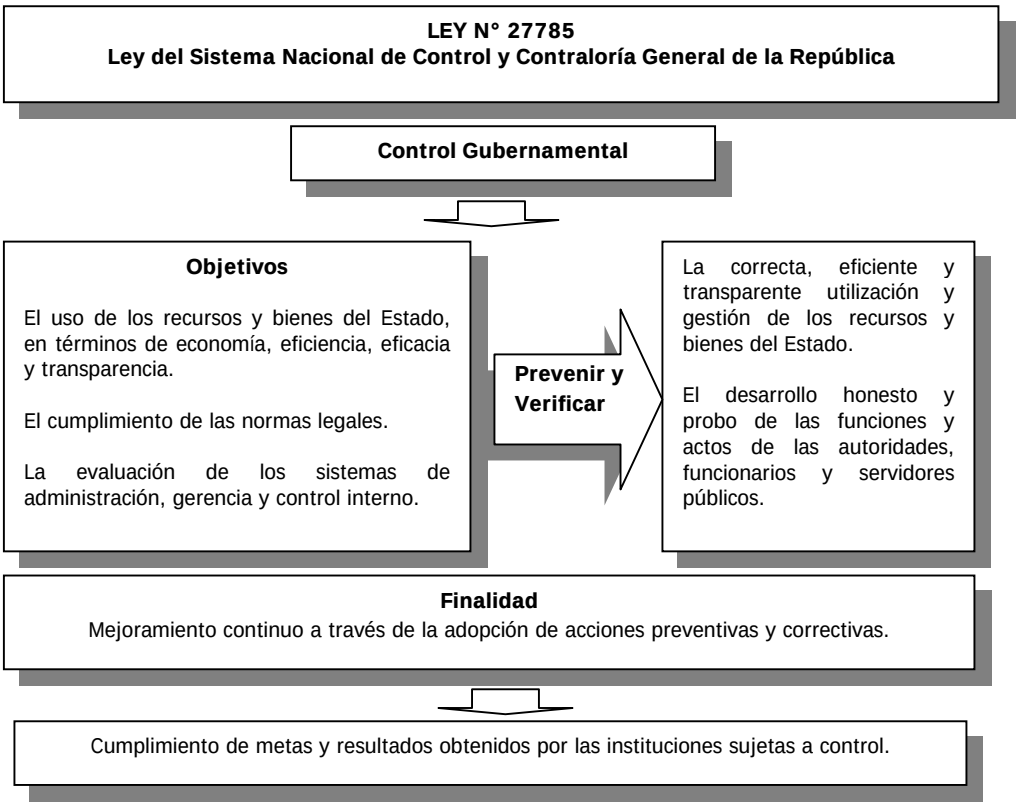
1.1.1.3. Control Gubernamental

Es un proceso continuo, permanente, dinámico e integral realizado por todos los trabajadores de la entidad que consiste en supervisar, vigilar y verificar (mediante la aplicación de principios, sistemas y procedimientos técnicos) los siguientes objetivos del control gubernamental dentro de la organización:

- El uso de los recursos y bienes del Estado, en términos de economía, eficiencia, eficacia y transparencia.
- El cumplimiento de las normas legales.
- La evaluación de los sistemas de administración, gerencia y control interno.

El control gubernamental tiene como finalidad el mejoramiento continuo a través de la adopción de acciones preventivas y correctivas, tal como se puede apreciar en el siguiente gráfico:

Gráfico N° 1.3. **Control Gubernamental**



El control gubernamental se clasifica en Interno y Externo:

a. Control Interno Gubernamental: Se subdivide en:

– Previo : Controles que se aplican antes que se ejecute el proceso.
– Simultáneo: Controles que se aplican durante el proceso.
– Posterior : Controles que se aplican después del proceso.

El control gubernamental 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.

El control gubernamental posterior es ejercido por los responsables superiores del servidor o funcionario ejecutor, en función del cumplimiento de las disposiciones establecidas, así como por el órgano de control institucional.

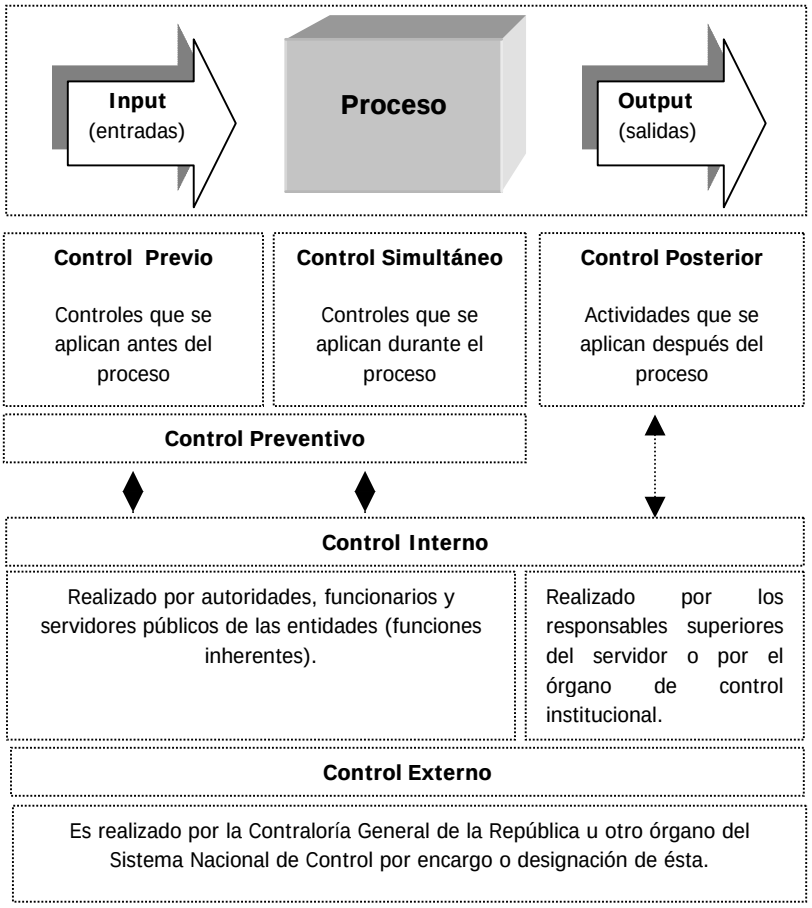
b. Control Externo Gubernamental: Se subdivide en:

– Previo : Controles que se aplican antes que se ejecute el proceso.
– Simultáneo: Controles que se aplican durante el proceso.
– Posterior : Controles que se aplican después del proceso.

El control externo gubernamental[1] es aplicado por la Contraloría General de la República u otro órgano del Sistema por encargo o designación de ésta.

Los tipos de control gubernamental, pueden ser apreciados en el siguiente gráfico:

Gráfico N° 1.4. **Tipos de Control Gubernamental**



[1] *El control externo podrá ser preventivo o simultáneo, cuando se determine taxativamente por la Ley N° 27785 o por normativa expresa.*

Las normas contenidas en la Ley N° 27785 y aquellas que emita la Contraloría General de la República son aplicables a todas las entidades sujetas a su ámbito de control, entre las cuales, tenemos a entidades de los Poderes Ejecutivo, unidades administrativas del Poder Judicial y Poder Legislativo, Organismos autónomos, Organismos reguladores, Gobiernos Locales y Regionales, las cuales se encuentran especificadas en el Art. 3 de la presente Ley.

1.1.2. Reglamento de los Órganos de Control Institucional

La Contraloría General de la República, mediante Resolución de Contraloría N° 459-2008-CG del 28.OCT.2008, aprobó el Reglamento de los Órganos de Control Institucional (OCI) el cual tiene por objetivo regular la actuación de los Órganos de Control Institucional en las entidades sujetas al Sistema Nacional de Control, la vinculación de dependencia administrativa y funcional del OCI y de su Jefe con la Contraloría General de la República así como sus funciones, obligaciones y atribuciones. La finalidad del Reglamento es fortalecer la labor del OCI y contribuir con el correcto ejercicio del control gubernamental.

Al respecto, el OCI es la unidad especializada responsable de llevar a cabo el control gubernamental, mediante la ejecución de labores de control; ubicándose en el mayor nivel jerárquico de la estructura de la entidad informando directamente al Titular de la entidad sobre los requerimientos y resultados de dichas labores de control. Al respecto, los Órganos de Control Institucional deberán estar conformados por personal multidisciplinario seleccionado en relación con los objetivos y actividades que realiza la entidad.

En ese sentido, el OCI ejercerá sus funciones sujeta a lo establecido en la Ley N° 27785 y a las normas emitidas por la Contraloría General. Entre sus principales funciones, se encuentran:

- Ejercer el control interno posterior a los actos y operaciones de la entidad sobre la base de los lineamientos y cumplimiento del Plan Anual de Control.
- Efectuar auditorías de conformidad con los lineamientos que emita la Contraloría General.
- Remitir los Informes resultantes de sus labores de control tanto a la Contraloría General como al Titular de la entidad.
- Formular, ejecutar y evaluar el Plan Anual de Control aprobado por la Contraloría General.
- Verificar el cumplimiento de las disposiciones legales y normativa interna aplicables a la entidad por parte de las unidades orgánicas y personal de ésta.

Asimismo, el OCI no puede realizar o intervenir en funciones y actividades inherentes al ámbito de competencia y responsabilidad de la administración y gestión de la entidad.

Es de significar, que la Contraloría General realiza supervisión permanente sobre el funcionamiento de los Órganos de Control Institucional.

1.1.3. Ley de Control Interno de las Entidades del Estado

La Ley N° 28716 del 17.ABR.2006 tiene por objeto establecer las normas para regular la implantación, funcionamiento, perfeccionamiento y evaluación del control interno en las entidades del Estado Peruano, con el propósito de cautelar y fortalecer los sistemas administrativos y operativos mediante acciones y actividades de control previo, simultáneo y posterior, con el fin de enfrentar los actos y prácticas indebidas o de corrupción, propendiendo al logro de los fines, objetivos y metas institucionales.

Al respecto, las normas establecidas en la Ley N° 28716 son de cumplimiento obligatorio a todas las entidades sujetas a control, las cuales son detalladas a continuación:

1.1.3.1. Sistema de Control Interno

Es el conjunto de acciones, actividades, planes, políticas, normas, registros, organización, procedimientos y métodos, incluyendo la actitud de las autoridades y el personal de las entidades del Estado.

a. Objetivos del Sistema de Control Interno: Son los siguientes:

1. Promover y optimizar la eficiencia, eficacia, transparencia y economía en las operaciones de la entidad, así como la calidad de sus servicios.
2. Cuidar y resguardar los recursos y bienes del Estado contra cualquier forma de pérdida, deterioro, uso indebido y actos ilegales, así como, contra todo acto que pudiera afectarlos.
3. Cumplir la normatividad aplicable a la entidad.
4. Garantizar la confiabilidad y oportunidad de la información.
5. Fomentar e impulsar la práctica de valores institucionales.
6. Promover la rendición de cuentas de los fondos y bienes públicos asignados a los funcionarios o servidores públicos.

b. Componentes del Sistema de Control Interno: Son los siguientes:

1. Ambiente de Control: Es el entorno organizacional favorable al ejercicio de prácticas, valores, conductas y reglas para el funcionamiento del control interno.

2. **Evaluación de Riesgos:** Consiste en identificar, analizar y administrar los eventos que puedan afectar adversamente el cumplimiento de los fines, metas, objetivos, actividades y operaciones institucionales.

3. **Actividades de Control Gerencial:** Son las políticas y procedimientos de control que imparte la dirección, gerencia y los niveles ejecutivos competentes, en relación con las funciones asignadas al personal.

4. **Actividades de Prevención y Monitoreo:** Son las acciones que deben ser adoptadas en el desempeño de las funciones asignadas, a fin de cuidar y asegurar su idoneidad y calidad.

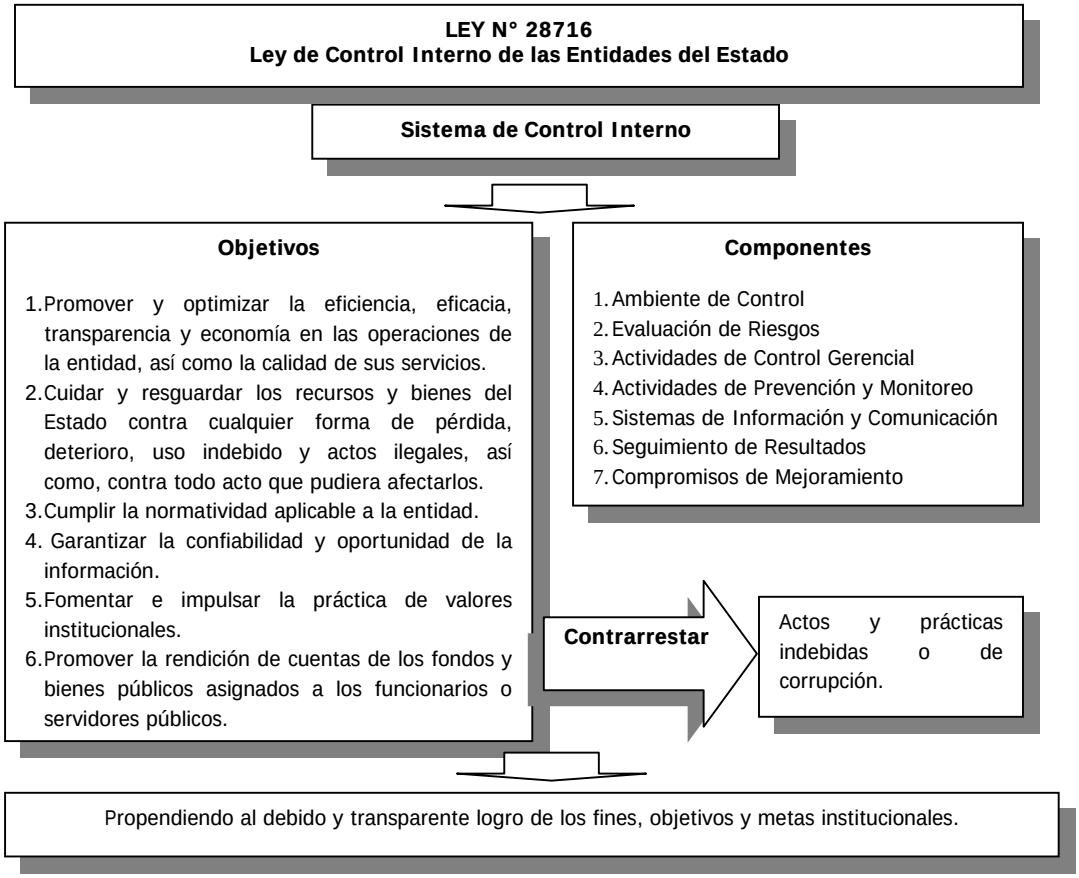
5. **Sistemas de Información y Comunicación:** Son los medios a través de los cuales el registro, procesamiento, integración y divulgación de la información (con bases de datos y soluciones informáticas) sirva para dar confiabilidad, transparencia y eficiencia a los procesos de gestión y control interno institucional.

6. **Seguimiento de Resultados:** Consiste en la revisión y verificación actualizada de las medidas de control interno implantadas, incluyendo la implementación de las recomendaciones formuladas en los informes emitidos por los órganos del Sistema Nacional de Control.

7. **Compromisos de Mejoramiento:** Incluye las autoevaluaciones realizadas por los órganos y personal de la administración institucional, conducentes al mejor desarrollo del control interno así como de informar sobre cualquier desviación o deficiencia susceptible de corrección.

En el siguiente gráfico se puede apreciar cómo interactúa el Sistema de Control Interno que debe ser implementado en cada una de las entidades públicas del Estado Peruano:

Gráfico N° 1.5. **Sistema de Control Interno**



Es responsabilidad del Sistema Nacional de Control (Contraloría General, Órganos de Control Institucional y Sociedades de Auditoría), la evaluación del sistema de control interno en las entidades del Estado, de conformidad con la normativa técnica del Sistema Nacional de Control Peruano.

La Contraloría General de la República ha emitido la normativa técnica de control (Normas de Control Interno) que orientan la efectiva implantación y funcionamiento del control interno en las entidades del Estado, así como su respectiva evaluación, la cuales son detallas a continuación:

1.1.4. Normas de Control Interno

La Resolución de Contraloría N° 320-2006-CG del 30.OCT.2006 tiene como objetivo el fortalecimiento de los Sistemas de Control Interno y el mejoramiento de la gestión pública de las entidades del Estado, considerando la protección del patrimonio público y el logro de los objetivos y metas institucionales.

Al respecto, las Normas de Control Interno son lineamientos, criterios y disposiciones para la aplicación y regulación del control interno en las principales áreas de la actividad administrativa u operativa de las entidades públicas promoviendo una administración adecuada de los recursos públicos.

Todo el personal de cada entidad es responsable de establecer, mantener, revisar y actualizar la estructura de control interno. Al respecto, el Órgano de Control Institucional de cada entidad forma parte del sistema de control interno.

Las Normas de Control Interno sirven de marco referencial en materia de control interno para la emisión de normativa específica de cada entidad, orientando y unificando la aplicación del control interno en las entidades del Estado sujetas a control gubernamental.

Cabe precisar que en el numeral 1 del rubro II referido al Marco Conceptual de la Estructura de Control Interno de la RC N° 320-2006-CG se hace mención a los mismos objetivos de control interno mencionados en la Ley N° 28716 – Ley de Control Interno de las Entidades del Estado.

1.1.4.1. Principios aplicables al Sistema de Control Interno

a. Autocontrol: El personal de cada entidad debe controlar su trabajo, detectar deficiencias y efectuar correctivos para el mejoramiento de sus labores y el logro de los resultados esperados.

b. Autorregulación: Capacidad institucional para desarrollar las disposiciones, métodos y procedimientos que le permitan cautelar, realizar y asegurar la eficacia, eficiencia, transparencia y legalidad en los resultados de sus procesos, actividades y operaciones.

c. Autogestión: Compete a cada entidad conducir, planificar, ejecutar, coordinar y evaluar las funciones a su cargo con sujeción a la normativa aplicable y objetivos previstos para su cumplimiento.

1.1.4.2. Componentes de la Estructura del Sistema de Control Interno

La estructura del Sistema de Control Interno está conformada por los siguientes cinco componentes, los cuales facilitan la implantación estandarizada de la estructura de control interno en las entidades del Estado:

a. Ambiente de Control
b. Evaluación de Riesgos
c. Actividades de Control
d. Sistemas de Información y Comunicación
e. Supervisión

Al respecto, los componentes (Ambiente de Control y Evaluación de Riesgos) conforman el Control Interno Estratégico, los componentes (Actividades de Control y Sistemas de Información) conformarían el Control Interno Operativo y por último el Componente Supervisión conformaría el Control Interno de Evaluación; los cuales se detallan a continuación:

a. Ambiente de Control: El Sistema de Control Interno debe contar con un entorno organizacional favorable al ejercicio de buenas prácticas, valores, conductas y reglas apropiadas, para sensibilizar a los miembros de la entidad y generar una cultura de control interno. Este componente está conformado por las siguientes ocho (8) normas:

1.1 Filosofía de la Dirección: Comprende la conducta y actitudes de la gestión de la entidad con respecto del control interno estableciendo un ambiente de confianza positivo y de apoyo hacia el control interno, por medio de una actitud abierta hacia el aprendizaje, innovación y transparencia.

1.2 Integridad y valores éticos: Se debe mantener una actitud de apoyo permanente hacia el control interno con base en la integridad y valores éticos establecidos en la entidad.

1.3 Administración estratégica: Consiste en planificar con componentes de misión, visión, metas y objetivos estratégicos.

1.4 Estructura organizacional: Consiste en desarrollar, aprobar y actualizar la estructura organizativa que contribuya al cumplimiento de los objetivos y misión de la entidad.

1.5 Administración de los recursos humanos: Consiste en establecer políticas y procedimientos para asegurar una

adecuada planificación y administración de los recursos humanos de la entidad.

1.6 Competencia profesional: La competencia profesional del personal, es un elemento importante en la entidad, el cual debe ser coherente con las funciones y responsabilidades asignadas.

1.7 Asignación de autoridad y responsabilidad: Consiste en asignar claramente al personal de la entidad sus deberes, responsabilidades y límites de autoridad.

1.8 Órgano de Control Institucional: El Órgano de Control Institucional, a través de actividades y acciones de control interno, contribuye a un adecuado ambiente de control.

b. Evaluación de Riesgos: El Sistema de Control Interno incluye la evaluación de riesgos como parte del proceso de administración de riesgos a los que está expuesta la entidad y que puede afectar el logro de sus objetivos. Este componente está conformado por las siguientes cuatro (4) normas:

2.1 Planeamiento de la Administración de riesgos: Es el proceso de elaborar una estrategia para identificar, valorar y dar respuesta a los riesgos que puedan impactar en una entidad, impidiendo el logro de los objetivos de la entidad.

2.2 Identificación de los riesgos: Consiste en tipificar todos los riesgos que pueden afectar el logro de los objetivos de la entidad debido a factores externos (económicos, medioambientales, políticos, sociales y tecnológicos) o internos (infraestructura, personal, procesos y tecnología).

2.3 Valoración de los riesgos: Consiste en analizar o valorar los riesgos potenciales que pueden afectar el logro de los objetivos de la entidad con el fin de estimar su probabilidad de ocurrencia e impacto.

2.4 Respuesta al riesgo: Consiste en identificar las diferentes opciones existentes con el fin de dar respuesta al riesgo, considerando su probabilidad de ocurrencia e impacto en relación con la tolerancia al riesgo que la entidad este dispuesta a sobrellevar en función de su costo-beneficio.

c. Actividades de Control Gerencial: El Sistema de Control Interno debe incluir políticas y procedimientos para asegurar que se están realizando las acciones necesarias que posibiliten una

adecuada respuesta a los riesgos que pueden afectar los objetivos de la entidad. Este componente está conformado por las siguientes diez (10) normas:

3.1 Procedimientos de autorización y aprobación: La responsabilidad por cada proceso, actividad o tarea organizacional debe estar claramente definida, específicamente asignada y formalmente comunicada al personal respectivo. Asimismo, la ejecución de los procesos, actividades, o tareas debe contar con la autorización y aprobación del personal con el rango de autoridad respectivo.

3.2 Segregación de funciones: Un solo cargo o equipo de trabajo no debe tener el control de todas las etapas clave en un proceso, actividad o tarea, con el fin de reducir los riesgos de error o fraude en los procesos, actividades o tareas.

3.3 Evaluación costo-beneficio: El diseño e implementación de las actividades o procedimientos de control deben ser precedidos por una evaluación de costo-beneficio considerando su factibilidad en relación con el logro de los objetivos de la entidad.

3.4 Controles sobre el acceso a los recursos o archivos: El acceso a los recursos o archivos debe estar limitado al personal autorizado, el cual debe estar sustentado en medios, que permitan llevar un adecuado control.

3.5 Verificaciones y Conciliaciones: Los procesos, actividades o tareas significativos deben ser verificados antes y después de realizarse. Asimismo, éstos deben ser registrados y clasificados para su revisión posterior.

3.6 Evaluación de desempeño: Consiste en una evaluación permanente de la gestión tomando como base los planes organizacionales y las disposiciones normativas vigentes, para prevenir y corregir cualquier deficiencia o irregularidad que se presente en la entidad.

3.7 Rendición de cuentas: La entidad así como su personal están obligados a rendir cuentas por el uso de los recursos y bienes del Estado así como el cumplimiento de la misión y objetivos institucionales.

3.8 Documentación de procesos, actividades y tareas: Los procesos, actividades y tareas deben estar documentados para

asegurar su adecuado desarrollo, facilitar la correcta revisión de los mismos y garantizar su trazabilidad.

3.9 Revisión de procesos, actividades y tareas: Los procesos, actividades y tareas deben ser periódicamente revisados para asegurar que cumplen con los reglamentos, políticas y procedimientos vigentes.

3.10 Controles para las Tecnologías de la Información y Comunicaciones (TIC): Las TIC abarcan datos, sistemas de información, tecnología asociada, instalaciones y el personal. Las actividades de control de las TIC incluyen controles que garanticen el procesamiento de la información para el cumplimiento de los objetivos de la entidad, debiendo estar diseñados para prevenir, detectar y corregir errores e irregularidades mientras la información fluye a través de los sistemas. Dichos controles son:

Controles Generales de TI: Los cuales afectan a toda la infraestructura de las tecnologías de información (infraestructura, personas, aplicaciones e información). Por tanto, estos controles son aplicables a todas las aplicaciones de TI.
Controles en los sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico.
Controles en la Segregación de funciones.
Controles de Acceso General, es decir, seguridad física y lógica de los equipos centrales.
Controles relacionados a la Continuidad en el servicio.

Controles de Aplicación: Son controles específicos de los sistemas de información en el ingreso, proceso y salida de la información; los cuales dan soporte a un proceso de negocio específico de la entidad a través de medios físicos o electrónicos.
Controles para el área de Desarrollo: - En el requerimiento, análisis, desarrollo, pruebas, pase a producción, mantenimiento y cambio en la aplicación del software. - En el aseguramiento de datos fuente por medio de accesos a usuarios internos del área de sistemas. - En la salida interna y externa de datos, por medio de documentación en soporte físico o electrónico o por medio de comunicaciones a través de publicidad y pagina web.
Controles para el área de Producción: - En la seguridad física, por medio de restricciones de acceso a la sala de cómputo y procesamiento de datos, a las redes instaladas, así como al respaldo de la información (backup). - En la seguridad lógica, por medio de la creación de perfiles de acuerdo con las funciones de los empleados, creación de usuarios con accesos propios (contraseñas) y relación de cada usuario con el perfil correspondiente.

Controles para el área de soporte técnico, en el mantenimiento de máquinas (hardware), licencias (software), sistemas operativos, utilitarios (antivirus) y bases de datos.

Los controles generales de TI y de aplicación están interrelacionados. Ambos resultan necesarios para garantizar la totalidad y exactitud del procesamiento de la información. Si el control general es inadecuado, es probable que el control de aplicación no funcione correctamente y pueda ser eludido. El control de aplicación supone que el control general funcionará adecuadamente e informará inmediatamente de los errores, incongruencias, formato incorrecto de los datos y acceso indebido a los mismos.

d. Información y Comunicación: El Sistema de Control Interno debe contar con métodos, procesos, canales y medios que permiten asegurar el flujo de información en todas las direcciones con el fin de cumplir con las responsabilidades individuales y grupales de la entidad. Este componente está conformado por las siguientes nueve (9) normas:

4.1 Funciones y características de la información: La información es el resultado de las actividades operativas, financieras y de control provenientes del interior o exterior de la entidad. Asimismo, considerando que dicha información es utilizada por el personal de la entidad en la ejecución de sus tareas operativas o de gestión, ésta debe reunir las características de confiabilidad, oportunidad y utilidad.

4.2 Información y responsabilidad: La información debe permitir al personal de la entidad cumplir con sus obligaciones y responsabilidades. Los datos necesarios deben ser captados, identificados, seleccionados, registrados, estructurados en información y comunicados en tiempo y forma oportuna.

4.3 Calidad y suficiencia de la información: Consiste en implementar mecanismos que aseguren la confiabilidad, calidad y oportunidad de la información que se genere y comunique en la entidad.

4.4 Sistemas de información: Los sistemas de información implementados por la entidad deben de ajustarse a sus necesidades. Dichos sistemas proveen de información para la toma de decisiones, facilitando y garantizando la transparencia

en la rendición de cuentas; contribuyendo de esta manera a alcanzar los objetivos que se ha trazado la entidad.

4.5 Flexibilidad al cambio: Los sistemas de información deben ser revisados periódicamente con el fin de que sean rediseñados cuando se detecten deficiencias en su funcionamiento, con el fin de que los sistemas de información estén alineados a los objetivos de la entidad.

4.6 Archivo institucional: La entidad debe establecer políticas y procedimientos de archivo adecuados para la preservación y conservación de la información y documentación de la entidad.

4.7 Comunicación interna: La comunicación interna es el flujo de mensajes que fluyen a través de la estructura interna de la entidad, con la finalidad de obtener un mensaje claro y eficaz para cada uno de los miembros de la organización.

4.8 Comunicación externa: La comunicación externa de la entidad debe asegurar que el flujo de mensajes e intercambio de información con los clientes, usuarios y ciudadanía, se lleve a cabo de manera segura, correcta y oportuna, generando una imagen positiva para a la entidad.

4.9 Canales de comunicación: Los canales de comunicación son medios diseñados de acuerdo con las necesidades de la entidad que permiten asegurar que la información llegue a cada destinatario en la cantidad, calidad y oportunidad requeridas que contribuyan a una mejor ejecución de los procesos de la entidad.

e. Supervisión: El Sistema de Control Interno debe ser objeto de supervisión para evaluar su funcionamiento en el tiempo y permitir su retroalimentación. Este componente está conformado por las siguientes seis (6) normas:

5.1. Normas Básica para las Actividades de Prevención y Monitoreo

5.1.1. Prevención y monitoreo: El monitoreo de los procesos y operaciones de la entidad debe permitir conocer si éstos se realizan de forma adecuada para el logro de sus objetivos y si se adoptan las acciones de prevención que permitan garantizar la calidad de dichos procesos.

5.1.2. Monitoreo oportuno del control interno: La implementación de las medidas de control interno sobre los procesos y operaciones de la entidad deben ser objeto de monitoreo oportuno, con el fin de efectuar las modificaciones necesarias que permitan asegurar su correcto funcionamiento.

5.2. Normas Básicas para el Seguimiento de Resultados

5.2.1. Reporte de deficiencias: Las deficiencias detectadas como resultado del proceso de monitoreo deben ser derivadas al personal responsable con el fin de que procedan a tomar acciones necesarias para su corrección.

5.2.2. Implantación y seguimiento de medidas correctivas: Cuando se detecten deficiencias que constituyan oportunidades de mejora (identificadas por la propia entidad o por los Órganos de Control Institucional), la entidad deberá adoptar las medidas correctivas y de seguimiento que permita asegurar que estas deficiencias sean corregidas.

5.3. Normas Básicas para los Compromisos de Mejoramiento

5.3.1. Autoevaluación: Se deben realizar ejecuciones periódicas de autoevaluación relacionadas al control interno de la entidad con el fin de verificar el estado situacional en que se encuentra la entidad y de está manera se establezca los compromisos de mejoramientos de la entidad.

5.3.2. Evaluaciones independientes: Las evaluaciones independientes deben de estar a cargo de los órganos de control competentes del Sistema Nacional de Control que permitan garantizar la verificación del sistema de control interno con el fin de formular recomendaciones que permitan corregir las deficiencias de control interno identificadas.

1.1.4.3. Limitaciones

La estructura del Sistema de Control Interno proporciona seguridad razonable sobre el logro de los objetivos trazados, presentándose las siguientes limitaciones:

a. Recursos Humanos:
   - Error de concepción, criterio, negligencia o corrupción.
   - Si el personal que realiza el control interno no entiende cual es su función en el proceso o decide ignorarlo, el control interno resultará ineficaz.

b. Recursos Materiales:
   - Debe considerarse los costos de los controles a implementar en función al beneficio que se obtendrá, producto de su implantación en la entidad.

1.1.5. Guía para la implementación del Sistema de Control Interno de las entidades del Estado

Mediante Resolución de Contraloría N° 458-2008-CG del 28.OCT.2008 se aprobó la"Guía para la Implementación del Sistema de Control Interno de las entidades del Estado", el cual tiene como objetivo el 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 establecido en las Normas de Control Interno con la finalidad que esta guía se constituya en un documento que permita una adecuada implementación del Sistema de Control Interno.

En ese sentido, es de significar que para la implementación de la norma de control interno 3.10 - Controles para las Tecnologías de la Información y Comunicaciones del Componente Actividades de Control Gerencial se menciona que debe tomarse en cuenta los estándares o buenas prácticas en Tecnologías de Información ya establecidas a nivel internacional a fin de desarrollar un marco propio que tome en cuenta la realidad de cada entidad, tales como:

- **COBIT** (Control OBjetives for Information and related Technology) es un marco de trabajo para el Gobierno de TI.

- **ITIL** (Information Technology Infrastructure Library) es un conjunto de prácticas para la gestión de servicios, desarrollo y operaciones de TI; para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI.

- **CMMI** (Capability Maturity Model Integration) es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de los sistemas de software.

- **ISO/IEC 27002:2005** (International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC)). Conocida anteriormente como ISO/IEC 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables para la gestión de la seguridad de la información.

1.1.6. Normas de Auditoría Gubernamental

La Contraloría General de la República aprobó, mediante Resolución de Contraloría N° 162-95-CG del 22.SET.1995, las Normas de Auditoría Gubernamental (NAGU) las cuales fueron formuladas tomando como base las Normas de Auditoría Generalmente Aceptadas (NAGA), Normas Internacionales de Auditoría (NIA), Normas de la Organización Internacional de Instituciones Supremas de Auditoría (INTOSAI) y Normas de auditoría emitidas por entidades homólogas.

Al respecto, las NAGU constituyen criterios generales orientados a uniformizar y optimizar los resultados del trabajo de auditoría gubernamental con el fin de obtener resultados de calidad. Dichas normas son de aplicación y cumplimiento obligatorio por parte del personal integrante de la Contraloría General de la República y de los Órganos de Auditoría Interna de las entidades sujetas al Sistema Nacional de Control, cuyo incumplimiento conlleva responsabilidad administrativa. Asimismo, la Contraloría General de la República se encargará de velar que los Órganos de Auditoría Interna cumplan con lo establecido en dichas normas gubernamentales.

Sobre el particular, las NAGU contribuyen a que las auditorías gubernamentales sean evaluaciones imparciales de la gestión gubernamental, contribuyendo a los objetivos institucionales de la entidad auditada.

1.1.6.1. Auditoría Gubernamental

La Auditoría Gubernamental es el examen objetivo, sistemático y profesional que se realiza a las operaciones financieras y/o administrativas de las entidades sujetas al Sistema Nacional de Control, efectuada con posterioridad a la ejecución de las operaciones de la entidad; la cual se materializa en el correspondiente informe de auditoría.

- Es objetiva, en la medida que la auditoría gubernamental considera que el auditor debe mantener una actitud independiente, respecto de las actividades a examinar en la entidad.
- Es sistemática, por cuanto la auditoría gubernamental responde a un proceso que es debidamente planificado.
- Es profesional, por cuanto la auditoría gubernamental es desarrollada por profesionales idóneos y expertos, sujetos a normas profesionales y al código de ética profesional.

Es de significar que la auditoría gubernamental es el medio utilizado para verificar que la gestión pública (operaciones financieras y/o administrativas) se haya realizado con economía, eficiencia, eficacia

y transparencia de conformidad con las disposiciones legales aplicables a la entidad auditada.

Asimismo, el auditor gubernamental es el profesional que se encarga de realizar las auditorías en las entidades sujetas al Sistema Nacional de Control utilizando las Normas de Auditoría Gubernamental y disposiciones especializadas emitidas por la Contraloría General.

En ese sentido, los auditores deben seleccionar y aplicar las pruebas y demás procedimientos de auditoría que, según su criterio profesional, sean apropiadas para cumplir los objetivos de cada auditoría. Esas pruebas y procedimientos deben planearse de tal modo que permitan obtener evidencia suficiente, competente y relevante para fundamentar razonablemente las conclusiones y recomendaciones que se formulen en los informes producto de las auditorías realizadas.

Es de significar, que la elaboración y presentación del informe de auditoría es de responsabilidad conjunta del auditor encargado y del supervisor que conforman la Comisión de Auditoría.

1.1.6.2. Objetivos de la Auditoría Gubernamental

- Evaluar el correcto uso de los recursos públicos, verificando el cumplimiento de las disposiciones legales y reglamentarias.
- Evaluar el grado en que se han alcanzado los objetivos de la entidad auditada en relación a los recursos asignados y los planes y programas aprobados.
- Evaluar la razonabilidad de la información financiera.
- Evaluar el sistema de control interno de la entidad auditada.
- Recomendar medidas para promover mejoras en la gestión pública.

1.1.6.3. Clasificación de la Auditoría Gubernamental

a. **Interna**: Es realizada por los Órganos de Auditoría Interna (o también llamados Órganos de Control Institucional) de las entidades sujetas al Sistema Nacional de Control.
b. **Externa:** Es realizada por la Contraloría General, Órganos de Auditoría Interna de otras entidades del Sistema Nacional de Control y por las Sociedades de Auditoría autorizadas por la Contraloría General.

1.1.6.4. Etapas de la Auditoría Gubernamental

a. Planificación
b. Ejecución

c. Elaboración del informe.

1.1.6.5. Tipos de Auditoría Gubernamental

a. Auditoría Financiera: Comprende la evaluación de los estados financieros de la entidad auditada, la cual tiene por objetivo determinar si los estados financieros de la entidad consignan razonablemente su situación financiera, tomando como referencia los principios de contabilidad generalmente aceptados.

Es de significar, que las Normas de Auditoría Generalmente Aceptadas (NAGA) y las Normas Internacionales de Auditoría NIA) son aplicables a la auditoría financiera.

b. Auditoría de Gestión: Comprende la evaluación del desempeño de la entidad auditada en relación al cumplimiento de las metas programadas y de los resultados obtenidos, con el fin de mejorar la efectividad, eficiencia y economía en el uso de los recursos públicos.

c. Examen Especial: Comprende la auditoría financiera y/o la auditoría de gestión, siendo su alcance menor al incluir solo la evaluación de una parte de las operaciones de la entidad a auditar. Asimismo, se efectúan exámenes especiales para evaluar, entre otros, el cumplimiento de los dispositivos legales, denuncias, procesos de adquisición de bienes o servicios públicos y cumplimiento de contratos de gestión gubernamental.

Cabe indicar que el Manual de Auditoría Gubernamental explica con mayor detalle los diferentes tipos de auditoría, entre ellos, el Examen Especial.

1.1.6.6. Conformación de las Normas de Auditoría Gubernamental

Están conformadas por 23 normas (integradas en 4 grupos) tal como se detalla a continuación:

a. Normas Generales.- Está conformado por las siguientes seis (6) normas:

1.10 Entrenamiento técnico y capacidad profesional: La auditoría gubernamental debe ser realizado por auditores gubernamentales que cuenten con la adecuada preparación en técnicas de auditoría así como un adecuado nivel de idoneidad y habilidad profesional.

1.20 Independencia: El auditor gubernamental tiene que tener una actitud de independencia respecto de la entidad auditada, absteniéndose de cualquier situación de incompatibilidad con el fin de asegurar una auditoria imparcial y objetiva.

1.30 Cuidado y esmero profesional: El auditor gubernamental debe aplicar correctamente los procedimientos que se hayan determinado para la realización de la auditoría gubernamental.

1.40 Confidencialidad: El auditor gubernamental debe mantener reserva durante todo el proceso de la auditoría gubernamental.

1.50 Participación de profesionales y/o especialistas: El personal profesional y/o especialista que ejercen sus actividades en campos diferentes a la auditoría gubernamental podrán integrar el equipo de auditoría en calidad de apoyo, cuando se considere necesario en la auditoría gubernamental.

1.60 Control de calidad: La auditoría gubernamental realizada por las entidades sujetas al Sistema Nacional de Control deben contar con un adecuado sistema de control de calidad, con el fin de proporcionar seguridad razonable de que las auditorías se realizan en función de las Normas de Auditoría Gubernamental, Manual de Auditoría Gubernamental y Guías de Auditoría Gubernamental.

b. Normas relativas a la Planificación de la Auditoría Gubernamental.- Está conformado por las siguientes cuatro (4) normas:

2.10 Planificación General: Mediante los Planes Anuales de Control, las entidades conformantes del Sistema Nacional de Control planifican las auditorías gubernamentales en función a las directivas establecidas por la Contraloría General de la República.

2.20 Planeamiento de la Auditoría: La auditoría gubernamental debe ser apropiadamente planificada. En dicho planeamiento se considera, entre otros, las actividades que realiza la entidad, su entorno y disposiciones legales.

2.30 Programas de auditoría: La auditoría gubernamental debe incluir programas de auditoría específicos que incluyan,

entre otros, los procedimientos a ejecutarse y personal encargado con el fin obtener evidencia competente, suficiente y relevante que sustente los objetivos de la auditoría.

2.40 Archivo permanente: Para cada entidad sujeta a control, se debe tener actualizado un archivo permanente con información básica de la entidad pública que se va a auditar.

c. Normas relativas a la Ejecución de la Auditoría Gubernamental.- Está conformado por las siguientes siete (7) normas:

3.10 Evaluación de la Estructura de Control Interno: La ejecución de la auditoría gubernamental incluye evaluar el control interno de la entidad a auditar con el fin de tomar conocimiento de los controles implementados y comprobar que estén funcionando correctamente, determinando el riesgo de control e identificación de áreas críticas.

3.20 Evaluación del cumplimiento de disposiciones legales y reglamentarias: La ejecución de la auditoría gubernamental incluye la evaluación del cumplimiento de la normativa aplicable a la entidad auditada.

3.30 Supervisión del trabajo de auditoría: La auditoría gubernamental debe ser supervisada durante todo su proceso, el cual consiste en controlar las actividades que son realizadas por el equipo de auditoría, con el fin de alcanzar los objetivos trazados; contribuyendo de esta manera a mejorar la calidad del informe de auditoría resultante.

3.40 Evidencia suficiente, competente y relevante: Durante la ejecución de la auditoría, el auditor gubernamental debe acreditar su trabajo, obteniendo evidencia (suficiente, competente y relevante); aplicando pruebas de control que fundamenten razonablemente el trabajo de auditoría.

3.50 Papeles de trabajo: El trabajo del auditor debe estar sustentado en un registro completo y detallado de las actividades realizadas en la auditoría gubernamental; dicho registro puede incluir medios de almacenamiento magnético, electrónico, informático u otro.

3.60 Comunicación de hallazgos: Producto del trabajo de campo realizado se comunican, de ser el caso, los hallazgos

obtenidos a las personas comprendidas en dichos hallazgos con el fin que puedan presentar sus aclaraciones o comentarios documentadamente para su correspondiente evaluación, lo cual será plasmado en el informe de auditoría.

3.70 Carta de representación: Durante la ejecución de la auditoría gubernamental, se debe obtener el documento (carta de representación) mediante el cual el titular y/o nivel gerencial competente de la entidad auditada comunica haber puesto a disposición de la Comisión de Auditoría la información solicitada y hechos significativos ocurridos durante el trabajo de campo de la auditoría.

d. Normas relativas al Informe de Auditoría Gubernamental.- Está conformado por las siguientes seis (6) normas:

4.10 Elaboración del informe: Concluido el trabajo de campo de la auditoría gubernamental, se procede a elaborar el informe de auditoría en el cual se presentan las deficiencias o desviaciones más significativas de la entidad auditada, así como, las recomendaciones que permitan mejorar su gestión, en concordancia a lo establecido en las Normas de Auditoria Gubernamental.

4.20 Oportunidad del informe: El informe de auditoría deberá se emitido en el plazo establecido en el programa de auditoría, con el fin que el contenido de informe de auditoría sea utilizado oportunamente por el titular de la entidad y/o autoridades del Estado para la respectiva toma de decisiones.

4.30 Características del informe: Los informes de auditoría deben emitirse considerando las siguientes características: calidad, concisión, exactitud y objetividad, de tal forma, que los hechos identificados durante el trabajo de campo de la auditoría gubernamental sean expuestos en un lenguaje sencillo y entendible.

4.40 Contenido del informe: En el informe de auditoría se deben exponer los resultados de la auditoría gubernamental en forma ordenada y adecuada, precisando que se efectuó en concordancia a las Normas de Auditoría Gubernamental.

4.50 Informe especial: Si en el trabajo de campo de la auditoría se evidencien indicios razonables de comisión de delito (responsabilidad penal) y/o perjuicio económico

(responsabilidad civil) se emitirá un informe especial, el cual debe estar técnica y legalmente sustentado.

4.60 Seguimiento de recomendaciones de auditorías anteriores: Las entidades que conforman el Sistema Nacional de Control deben efectuar el seguimiento que permita verificar que las entidades auditadas han implementado las recomendaciones de informes de auditorías anteriores.

1.1.6.7. Modificatorias de las Normas de Auditoría Gubernamental

En el siguiente cuadro se muestra las cinco (05) modificatorias que ha tenido la Resolución de Contraloría N° 162-95-CG del 22.SET.1995 que aprueba las Normas de Auditoría Gubernamental.

Normas de Auditoría Gubernamental (NAGU)		**Modificatorias a la RC N° 162-95-CG del 22.SET.1995**				
		RC N° 141-99-CG (25.NOV.1999)	RC N° 259-2000-CG (07.DIC.2000)	RC N° 12-2002-CG (21.ENE.2002)	RC N° 89-2002-CG (09.MAY.2002)	RC N° 309-2011-CG (28.OCT.2011)
1.10	Entrenamiento Técnico y Capacidad Profesional	-	-	-	-	-
1.20	Independencia	-	-	-	-	-
1.30	Cuidado y Esmero Profesional	-	-	-	-	-
1.40	Confidencialidad	-	-	-	-	-
1.50	Participación de Profesionales y/o Especialistas	-	-	-	-	-
1.60	Control de Calidad	√	-	-	-	-
2.10	Planificación General	-	-	-	-	-
2.20	Planificación Específica	√	-	-	-	-
2.30	Programas de Auditoría	√	-	-	-	-
2.40	Archivo Permanente	√	-	-	-	-
3.10	Estudio y Evaluación del Control Interno	√	√	-	-	√
3.20	Evaluación del Cumplimiento de Disposiciones Legales y Reglamentarias	√	-	-	-	-
3.30	Supervisión del Trabajo de Auditoría	√	-	-	-	-
3.40	Evidencia Suficiente, Competente y Relevante	√	-	-	-	√
3.50	Papeles de Trabajo	√	-	-	-	-
3.60	Comunicación de Observaciones	√	√	-	-	-
3.70	Carta de Representación	-	-	-	-	-
4.10	Forma Escrita	-	√	-	-	√
4.20	Oportunidad del Informe	-	√	-	-	-
4.30	Presentación del Informe	-	√	-	-	-
4.40	Contenido del Informe	√	√	-	-	√
4.50	Informe Especial	√	√	√	√√√	-
4.60	Seguimiento de Recomendaciones de Auditorías Anteriores	√√	-	-	-	√

(√) : Sustitución Total de Norma
(√√) : Incorporación de Norma
(√√√) : Sustitución Parcial de Norma

1.1.7. Manual de Auditoría Gubernamental

La Contraloría General de la República aprobó, mediante Resolución de Contraloría N° 152-98-CG del 18.DIC.1998, el Manual de Auditoría Gubernamental (MAGU), habiendo tomado como criterios y fundamentos las Normas de Auditoría Gubernamental (NAGU), Normas de Auditoría Generalmente Aceptadas (NAGA), Normas Internacionales de Auditoría aprobadas por el INTOSAI, Normas Internacionales de Auditoría (NIA) aprobadas por el Comité Internacional de Prácticas de Auditoría de la Federación Internacional de Contadores (IFAC), Declaraciones sobre Normas de Auditoría publicadas por el Instituto Americano de Contadores Públicos (AICPA), Pronunciamientos del Colegio de Contadores Públicos de Lima, Normas de Auditoría Gubernamental aprobadas por la Contraloría General de los Estados Unidos de América (GAO) y Directrices de Control Interno aprobadas por el INTOSAI.

El Manual de Auditoría Gubernamental es el documento normativo aplicable al Sistema Nacional de Control Peruano, en el cual se definen las políticas y lineamientos de la auditoría gubernamental, sus objetivos son los siguientes:

- Establecer la metodología de la auditoría gubernamental, con el propósito de uniformizar el trabajo de los auditores.
- Determinar los criterios que permitan llevar a cabo el control de calidad de la auditoría gubernamental.
- Aplicar las Normas de Auditoría Gubernamental (NAGU) así como la normatividad que sea aplicable a la entidad auditada.
- Proporcionar un medio de consulta para el personal que ejerce la auditoría gubernamental.

1.1.7.1. Postulados básicos de la auditoría gubernamental: Son premisas que sirven de soporte a las opiniones de los auditores gubernamentales en sus informes de auditoría, asimismo, son utilizadas cuando no existen normas específicas aplicables. Dichos postulados son los siguientes:

- Autoridad legal para ejercer la auditoría gubernamental, es decir, la Controlaría General de la República en su calidad de ente rector del Sistema Nacional de Control emite la normativa que regula el ejercicio de la auditoría gubernamental.
- Aplicabilidad de las normas de auditoría gubernamental, comprende la obligación de su cumplimiento por parte del personal de la Contraloría General de la República, Órganos de Auditoría Interna (Oficinas de Control Institucional) y Sociedades de Auditoría designadas por la Contraloría.

- Importancia relativa, relacionado a la magnitud o naturaleza de un monto erróneo. Asimismo, un asunto es de importancia relativa si su conocimiento puede tener consecuencias para el destinatario del informe de auditoría.
- La auditoría gubernamental se dirige a la mejora de las operaciones futuras, las cuales están materializadas en las recomendaciones producto de los informes de auditoría, en vez de criticar solamente las situaciones identificadas en el pasado, producto de la auditoría realizada.
- Juicio imparcial de los auditores, el cual está relacionado a la objetividad con la que debe realizarse la auditoria gubernamental.
- Obligaciones profesionales a los auditores. La auditoría gubernamental impone obligaciones profesionales a los auditores, las cuales deben estar sustentadas en el código de ética del auditor gubernamental.
- Acceso a todo tipo de información pública comprende el acceso a la información en cualquier momento y sin ningún tipo de limitación, aún cuando esta información sea secreta.
- Aplicación de la materialidad en la auditoría gubernamental comprende en priorizar la evaluación de las operaciones más significativas de la entidad, enfatizando su evaluación en los problemas más importantes de la entidad auditada.
- Perfeccionamiento de los métodos y técnicas de auditoría.
- Existencia de controles internos apropiados, está relacionado a que la entidad pública implemente y mantenga un sistema de control interno sólido que permita minimizar irregularidades, lo cual no implica que dicho sistema sea perfecto, sin embargo, sí permite minimizarlos. Al respecto, el auditor gubernamental tiene la responsabilidad de identificar dichas debilidades de control.
- Las operaciones y contratos gubernamentales, están libres de irregularidades y actos de colusión, es decir, se asume como premisa que personal de las entidades públicas son honestos, salvo prueba en contrario.
- Respondabilidad comprende la obligación de rendir cuenta por parte del personal o entidades públicas que manejan recursos públicos.

Respecto de los Postulados mencionados es de resaltar el relacionado al de Perfeccionamiento de los métodos y técnicas de auditoría, en el cual textualmente se establece lo siguiente: *"...La Importancia del rol que vienen adquiriendo los auditores exige de ellos el perfeccionamiento y la elaboración de nuevas metodologías, así como las técnicas para determinar si la entidad auditada aplica criterios razonables, en la evaluación de su desempeño operativo..."*. Sobre el particular, el presente trabajo de tesis contribuye con presentar una propuesta

metodológica que permita guiar las auditorías gubernamentales en temas de carácter informático.

1.1.7.2. Criterios básicos aplicables a la auditoría gubernamental: Son lineamientos generales que aseguran la uniformidad en las tareas que realizan los auditores gubernamentales en términos de eficiencia, efectividad y economía con el fin de proporcionar seguridad razonable de que se están logrando los objetivos y metas programados. Dichos criterios son los siguientes:

- Eficiencia en el manejo de la auditoría gubernamental, con el fin de orientar los recursos de la Contraloría hacia entidades en las que se puedan lograr mejoras importantes.
- Entrenamiento continuo, con el fin de que exista un entrenamiento continuo de auditor gubernamental que lo mantenga en altos niveles de capacidad profesional.
- Conducta funcional del auditor gubernamental, relacionada a la conducta intachable y reglas de conducta que debe seguir el auditor gubernamental.
- Alcance de la auditoría, implica la selección de áreas o asuntos que serán evaluados durante la auditoría gubernamental.
- Comprensión y conocimiento de la entidad a ser auditada.
- Comprensión de la estructura de control interno de la entidad a ser auditada.
- Utilización de especialistas en la auditoría gubernamental, dependiendo de la complejidad de la auditoría se solicitará la participación de profesionales especializados que brinden el asesoramiento técnico necesario.
- Detección de irregularidades o actos ilícitos, la auditoría gubernamental debe considerar procedimientos que ofrezcan garantía razonable para la detección de irregularidades o actos ilícitos que pudieran repercutir sobre la entidad auditada.
- Reconocimiento de logros notables de la entidad, es importante reconocer en los informes de auditoría los logros notables efectuados por la entidad, ya que pueden ser aplicables a otras entidades públicas.
- Comunicación oportuna de los resultados de la auditoría, con el fin de que la entidad auditada adopte las medidas correctivas pertinentes producto de las recomendaciones realizadas en los informes de auditoría.
- Comentarios de los funcionarios de la entidad auditada, este criterio está relacionado a los documentos de respuestas de los auditados a los hallazgos u observaciones identificados durante el trabajo de campo, los cuales deben formar parte del informe de auditoría.

- Presentación del borrador del informe a la entidad auditada, con el fin de que dicho documento sea revisado y comentado previamente por los responsables de la entidad auditada.
- Calidad de los informes de auditoría, es decir, los informes de auditoría deben ser, entre otros, oportunos, exactos, claros, objetivos y precisos.
- Tono constructivo en la auditoría, las actividades que se realicen durante la auditoría gubernamental deben ser tratados de manera positiva y constructiva.
- Organización de los informes de auditoría, cada informe de auditoría gubernamental debe organizarse apropiadamente en función a lo informado en dicho informe.
- Revisiones de control de calidad en las Auditorías Internas, es un proceso técnico que consiste en verificar el cumplimiento de la normativa emitida por la Contraloría General de la República.
- Transparencia de los informes de auditoría, los informes de auditoría deben estar en lo posible a disposición del personal que por razones de función o conocimiento general tengan interés en conocerlos.
- Acceso de personas a documentos sustentatorios de la auditoría, este criterio está relacionado al requerimiento de los funcionarios públicos de poder acceder a papeles de trabajo que sustentan las observaciones que figuran en el informe de auditoría.

1.1.7.3. Funciones del personal conformante de la auditoría gubernamental

Las funciones del Supervisor, Auditor Encargado y Personal de Auditoría son las siguientes:

a. Responsabilidades del Supervisor: El Supervisor asiste a los niveles gerenciales respecto a temas relacionados a la auditoría gubernamental; siendo sus responsabilidades las siguientes:

- Revisar y aprobar los procedimientos de auditoría planeados, establecidos en el Programa de Auditoría, antes del comienzo del trabajo de campo.
- Programar el personal profesional que participará de la auditoría.
- Vigilar el progreso de la auditoría, lo cual incluye el tiempo y costos de la auditoría.
- Solucionar los problemas identificados por el Auditor Encargado y el Personal de Auditoría.
- Supervisar y asesorar al Auditor Encargado, así como orientar a otros miembros del Personal de Auditoría.
- Supervisar la elaboración del Informe de Auditoría.
- Revisar los papeles de trabajo de la auditoría.
- Cautelar el cumplimiento de las NAGU y MAGU.

b. Responsabilidades del Auditor Encargado: El Auditor Encargado trabaja con el personal de auditoría en la entidad auditada administrando el trabajo de campo y desarrollando los procedimientos de auditoría; siendo sus responsabilidades las siguientes:

- Preparar la fase de planeamiento.
- Identificar los problemas de auditoría para coordinarlos con el Supervisor.
- Supervisar, asesorar y asistir al personal de auditoría con el fin que se comprendan los objetivos de la auditoría.
- Revisar los papeles de trabajo que prepare el Personal de Auditoría evaluando la evidencia obtenida.
- Redactar el informe de auditoría.
- Cumplir y hacer cumplir las NAGU y MAGU.

a. Responsabilidades del Personal de Auditoría: El Personal de Auditoría es responsable de desempeñar el trabajo que el Auditor Encargado le encargue; siendo sus responsabilidades las siguientes:

- Comprender y realizar los procedimientos de auditoría asignados.
- Elaborar los papeles de trabajo.
- Informar al Auditor Encargado sobre asuntos o problemas que se detecten.
- Formular sugerencias para mejorar la metodología y el desarrollo de la auditoría.
- Cumplir las NAGU y MAGU.

1.1.7.4. Examen Especial: Este tipo de auditoría gubernamental está integradas por las fases de Planeamiento, Ejecución y Elaboración de Informe. Cabe precisar que las Normas de Auditoría son aplicables a dichas fases.

a. Planeamiento: Está fase comprende lo siguiente:
- Entender los aspectos identificados que serán objeto del Examen Especial
- Identificar las líneas de autoridad y responsabilidad.
- Identificar el marco legal y normas reglamentarias aplicables.

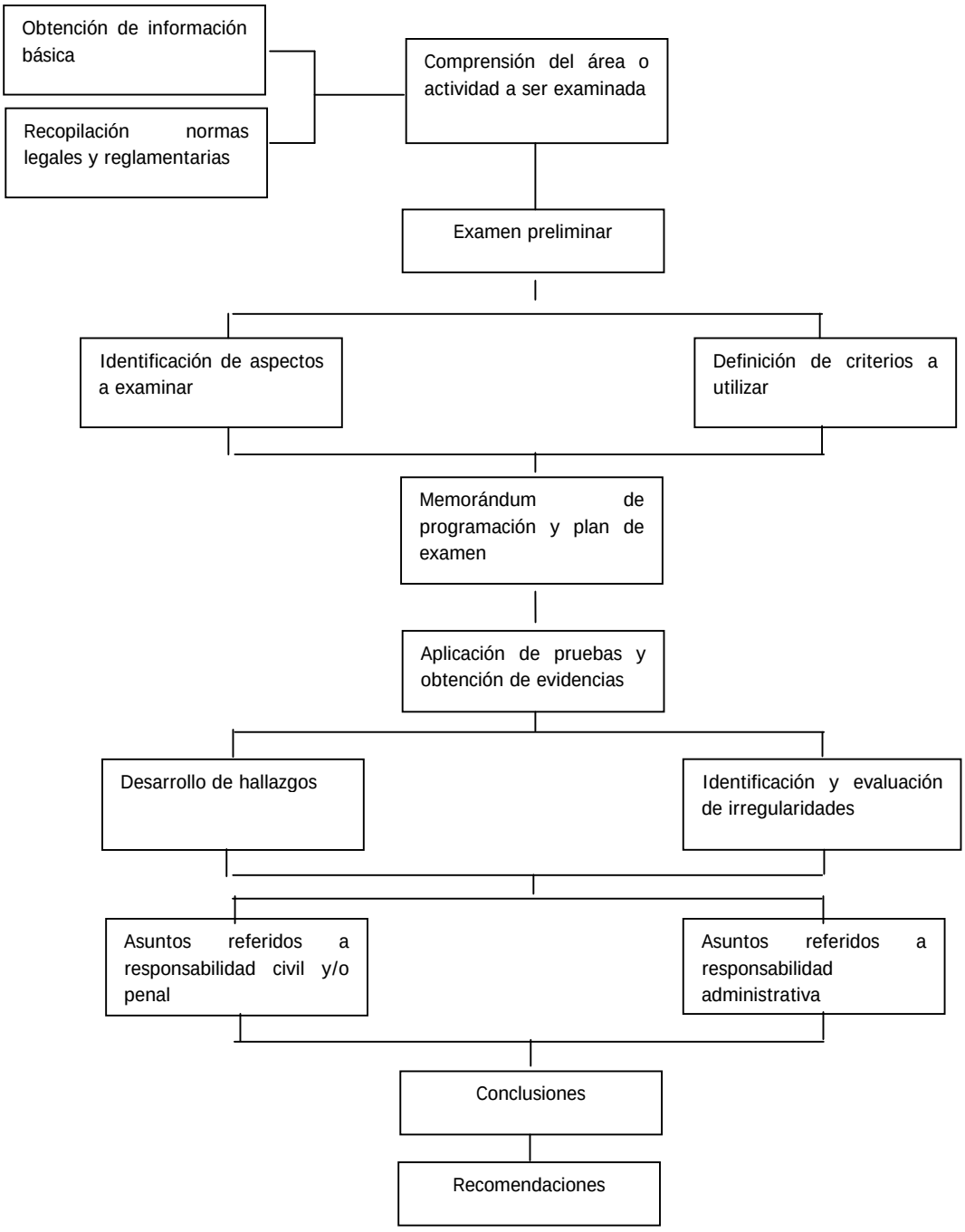
b. Ejecución: Está fase comprende lo siguiente:
- Aplicar pruebas de auditoría que permitan obtener evidencia suficiente, competente y pertinente que sustenten los hallazgos identificados.

- Si en el transcurso de la fase de ejecución se determinan situaciones de indicios razonables de comisión de delito se debe establecer el tipo de responsabilidad que corresponde a los presuntos implicados.

c. Elaboración del informe: Representa el producto final de la auditoría gubernamental que incluye las conclusiones y recomendaciones debidamente fundamentadas, producto del trabajo de campo realizado.

A continuación, en el siguiente gráfico se puede apreciar las actividades que conforman el proceso de auditoría del Examen Especial:

Gráfico N° 1.6. **Proceso de Auditoría del Examen Especial**



Fuente: Manual de Auditoría Gubernamental

1.1.7.5. Controles relativos al Sistema de Información Computarizada (SIC)

Se ha identificado en el Apéndice 5 del Manual de Auditoría Gubernamental (MAGU) que los controles relativos al Sistema de Información Computarizado están clasificados en Controles Generales, Controles de Aplicaciones y Controles de Usuarios, tal como se detalla a continuación:

a. Controles Generales: Son políticas y procedimientos que se aplican a la totalidad de las operaciones computarizadas de una entidad, creando el medio en el cual se aplican los controles de aplicación y de usuario. Dichos controles se subdividen en:

Organización y Segregación de Funciones: Son controles generales relacionados a la organización del Sistema de Información Computarizado. Al respecto, dichos controles incluyen lo siguiente:

- El procesamiento de información debe ser realizado por personal autorizado y debidamente supervisado.
- La segregación de funciones debe ser apropiada.
- Realizar un seguimiento de las recomendaciones efectuadas durante las revisiones internas y externas realizadas a las operaciones computarizadas.

Diseño de sistemas, desarrollo y modificación: Son controles generales que incluyen lo siguiente:

- Las modificaciones realizadas a los sistemas informáticos deben ser debidamente autorizadas y aprobadas cumpliendo los procedimientos de prueba establecidos.
- Se deben usar las metodologías de desarrollo y mantenimiento de sistemas.
- Se debe considerar a los usuarios como parte integral del desarrollo y mantenimiento de sistemas.

Seguridad: Los controles generales de seguridad proveen la certeza que los recursos computarizados están protegidos en contra del acceso físico y lógico no autorizado, pérdida o deterioro. Al respecto, dichos controles incluyen lo siguiente:

- Proteger a la entidad de la pérdida de recursos computarizados, debido a robo, destrucción, desastres naturales u otros medios.
- Limitar el impacto de pérdidas de recursos computarizados.

b. **Controles de Aplicaciones:** Son controles específicos que son incorporados en cada una de las aplicaciones informáticas para proveer seguridad razonable en el ingreso, procesamiento y salida de datos.

c. **Controles de Usuarios**: Son comparaciones manuales realizadas por el usuario, que consiste en comparar la información procesada por el sistema informático y la información procesada por el propio usuario.

1.1.7.6. Modificatorias del Manual de Auditoría Gubernamental

Mediante Resolución de Contraloría N° 141-99-CG del 25.NOV.1999 se modificaron los numerales 9, 10 y 11 del rubro 275 - Actos ilegales detectados en la entidad auditada correspondiente a la Fase de Ejecución de la Auditoría Financiera así como los numerales 25 y 28 del rubro 730 correspondiente a la Fase de Ejecución del Examen Especial.

1.1.8. Cuadros Comparativos

A continuación se muestran tres cuadros comparativos relacionados a la normatividad que se ha descrito en los numerales anteriores del presente trabajo de tesis:

- Ley N° 27785 del 22.JUL.2002: Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.
- Ley N° 28716 del 17.ABR.2006: Ley de Control Interno de las Entidades del Estado.
- Resolución de Contraloría N° 459-2008-CG del 28.OCT.2008: Reglamento de los Órganos de Control Institucional.
- Resolución de Contraloría N° 320-2006-CG del 30.OCT.2006: Normas de Control Interno.
- Resolución de Contraloría N° 458-2008-CG del 28.OCT.2008: Guía para la implementación del Sistema de Control Interno de las entidades del Estado.
- Resolución de Contraloría N° 162-95-CG del 22.SET.1995: Normas de Auditoría Gubernamental.
- Resolución de Contraloría N° 152-98-CG del 18.DIC.1998: Manual de de Auditoría Gubernamental.

1.1.8.1. Cuadro Comparativo entre las Leyes N° 27785, Ley 28716, Resoluciones de Contraloría N° 459-2008-CG, 320-2006-CG, 458-2008-CG, 162-95-CG y 152-98-CG referidos a los objetivos y finalidad de cada normativa

En el siguiente cuadro comparativo se puede apreciar los objetivos de cada una de las normas evaluadas:

Normativa	Fecha	Sumilla	Objetivo	Finalidad
Ley N° 27785	22.JUL.2002	Ley Orgánica del SNC y de la CGR	Obtener un apropiado, oportuno y efectivo ejercicio del control gubernamental.	Contribuir al mejoramiento de las actividades y servicios de la entidad pública en beneficio del país.
RC N° 459-2008-CG	28.OCT.2008	Reglamento de los OCI	Regular la actuación de los OCI, la vinculación de dependencia administrativa y funcional del OCI y de su Jefe con la CGR así como sus funciones, obligaciones y atribuciones.	Fortalecer la labor del OCI y contribuir con el correcto ejercicio del control gubernamental.
Ley N° 28716	17.ABR.2006	Ley de Control Interno de las Entidades del Estado	Establecer las normas para regular la implantación, funcionamiento, perfeccionamiento y evaluación del control interno en las entidades del Estado, con el propósito de cautelar y fortalecer los sistemas administrativos y operativos mediante acciones y actividades de control previo, simultáneo y posterior, con el fin de enfrentar los actos y prácticas indebidas o de corrupción, propendiendo al logro de los fines, objetivos y metas institucionales	
RC N° 320-2006-CG	30.OCT.2006	Normas de Control Interno	Fortalecimiento de los SCI y el mejoramiento de la gestión pública de las entidades del Estado, considerando la protección del patrimonio público y el logro de los objetivos y metas institucionales.	

RC N° 458-2008-CG	28.OCT.2008	Guía para la implementación del SCI	Proveer de lineamientos, herramientas y métodos a las entidades del Estado para la implementación de los componentes que conforman el SCI establecido en las NCI	Permitir una adecuada implementación del SCI.
RC N° 162-95-CG	22.SET.1995	NAGU	Uniformizar y optimizar los resultados del trabajo de auditoría gubernamental con el fin de obtener resultados de calidad.	
RC N° 152-98-CG	18.DIC.1998	MAGU	Establecer la metodología de la auditoría gubernamental, con el propósito de uniformizar el trabajo de los auditores.	

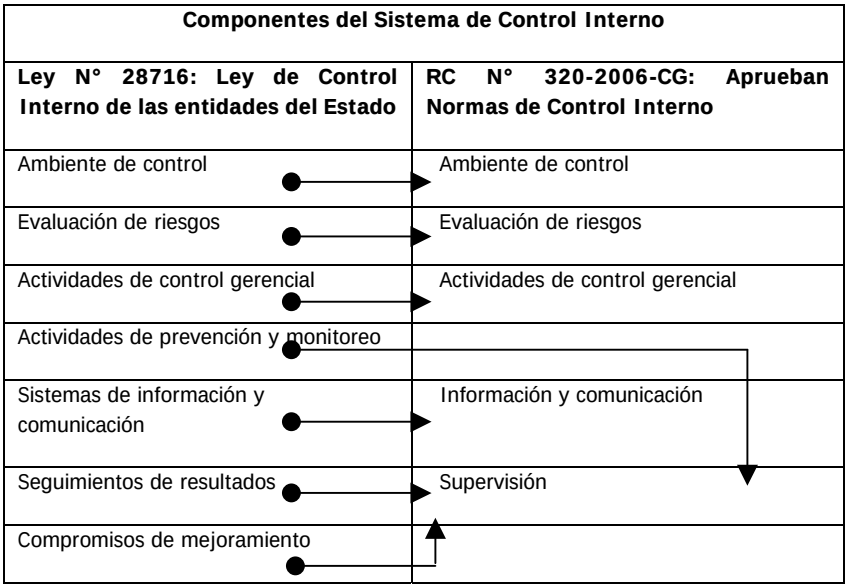
1.1.8.2. Cuadro Comparativo entre la Ley N° 27785 referido a los Objetivos de Control Gubernamental y la Ley N° 28716 referido a los Objetivos del Control Interno Gubernamental

En el siguiente cuadro comparativo se puede apreciar que la Ley N° 27785 - Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República considera 4 objetivos de control gubernamental, mientras que la Ley N° 28716 - Ley de Control Interno de las Entidades del Estado considera 6 objetivos circunscritos al control interno gubernamental, debiendo precisarse que los objetivos de la Ley N° 28716 se establecen a partir de los normados en la Ley N° 27785, tal como se muestra a continuación:

Ley N° 27785: Ley Orgánica del Sistema Nacional de Control y de la CGR (Control Gubernamental)	**Ley N° 28716: Ley de Control Interno de las entidades del Estado (Control Interno Gubernamental)**
22.JUL.2002	**17.ABR.2006**
El uso de los recursos y bienes del Estado, en términos de economía, eficiencia, eficacia y transparencia.	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.
	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.
El cumplimiento de las normas legales.	Cumplir la normatividad aplicable a la entidad y sus operaciones.
La evaluación de los sistemas de administración, gerencia y control interno.	Garantizar la confiabilidad y oportunidad de la información.
	Fomentar e impulsar la práctica de valores institucionales.
	Promover el cumplimiento de los funcionarios o servidores públicos de rendir cuenta por los fondos y bienes públicos a su cargo o por una misión u objetivo encargado y aceptado

1.1.8.3. Cuadro Comparativo entre la Ley N° 28716 y la RC N° 320-2006 referido a los Componentes del Sistema de Control Interno

En el siguiente cuadro comparativo se puede apreciar que la Ley N° 28716 - Ley de Control Interno de las Entidades del Estado considera 7 componentes del Sistema de Control Interno, mientras que la Resolución de Contraloría N° 320-2006-CG que aprueba las Normas de Control Interno considera 5 componentes, debiendo precisarse que los componentes de la RC N° 320-2006-CG se establecen a partir de los normados en la Ley N° 28716, tal como se muestra a continuación:



Por otro lado, es de significar que las principales normas emitidas por el Congreso Peruano y que son aplicables al Sistema Nacional de Control Peruano se encuentran en el **Anexo N° 1** del presente trabajo de tesis. Asimismo, en **Anexo N° 2** se encuentra la normatividad emitida por la Contraloría General de la República y que son aplicables al presente trabajo de tesis.

1.2. Normativa relacionada a la Oficina Nacional de Gobierno Electrónico e Informática

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) es el ente rector del Sistema Nacional de Informática[2]. Dicha oficina forma parte de la Presidencia del Consejo de Ministros (PCM) la cual tiene como funciones, entre otros, las que se indican a continuación:

- Aprobar los estándares tecnológicos relacionados a las medidas de seguridad de la información en las entidades públicas.
- Brindar asistencia técnica a las entidades públicas para la implementación de proyectos tecnológicos.
- Formular propuestas para impulsar el proceso de desarrollo e innovación tecnológica para la mejora y modernización de la gestión pública.

Sobre el particular, mediante Resolución Ministerial N° 246-2007-PCM del 22.AGO.2007, la Presidencia del Consejo de Ministros aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI Tecnología 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. Cabe resaltar que dicha Norma Técnica Peruana se basa en el estándar internacional ISO/IEC 27002:2005[3].

La NTP-ISO/IEC 17799:2007 se encuentra conformada por 11 Cláusulas, 39 Categorías y 133 controles. En el siguiente cuadro se puede apreciar dichas clausulas y categorías; mientras que el detalle de los 133 controles se puede apreciar en el **Anexo N° 3** del presente trabajo de tesis.

Cuadro de la NTP-ISO/IEC 17799:2007

CLÁUSULAS y CATEGORÍAS							
5. Política de Seguridad		**6. Aspectos organizativos para la seguridad**		**7. Clasificación y control de activos**		**8. Seguridad en recursos humanos**	
5.1	Política de seguridad de la información	6.1	Organización interna	7.1	Responsabilidad sobre los activos	8.1	Seguridad antes del empleo
		6.2	Seguridad en los accesos de terceras partes	7.2	Clasificación de la información	8.2	Durante el empleo
						8.3	Finalización o cambio del empleo

[2] *Creado mediante Decreto Legislativo N° 604 del 30.ABR.1990 con el fin de organizar las actividades y proyectos que en materia de informática realizan las entidades del Estado Peruano; está conformado, entre otros, por las oficinas informáticas públicas.*

[3] *El estándar ISO/IEC 17799:2005 posteriormente cambio de nombre convirtiéndose en estándar internacional ISO/IEC 27002:2005*

9. Seguridad física y del entorno		10. Gestión de comunicaciones y operaciones		11. Control de accesos		12. Adquisición, desarrollo y mantenimiento de sistemas	
9.1	Áreas seguras	10.1	Procedimientos y responsabilidades de operación	11.1	Requisitos de negocio para el control de accesos	12.1	Requisitos de seguridad de los sistemas
9.2	Seguridad de los equipos	10.2	Gestión de servicios externos	11.2	Gestión de acceso de usuarios	12.2	Seguridad de las aplicaciones del sistema
		10.3	Planificación y aceptación del sistema	11.3	Responsabilidades de los usuarios	12.3	Controles criptográficos
		10.4	Protección contra software malicioso	11.4	Control de acceso a la red	12.4	Seguridad de los archivos del sistema
		10.5	Gestión de respaldo y recuperación	11.5	Control de acceso al sistema operativo	12.5	Seguridad en los procesos de desarrollo y soporte
		10.6	Gestión de seguridad en redes	11.6	Control de acceso a las aplicaciones y la información	12.6	Gestión de la vulnerabilidad técnica
		10.7	Utilización de los medios de información	11.7	Informática móvil y teletrabajo		
		10.8	Intercambio de información				
		10.9	Servicios de correo electrónico				
		10.10	Monitoreo				

CLAUSULAS y CATEGORÍAS					
13. Gestión de incidentes en la seguridad de información		14. Gestión de continuidad del negocio		15. Cumplimiento	
13.1	Reportando eventos y debilidades de la seguridad de información	14.1	Aspectos de la gestión de continuidad del negocio	15.1	Cumplimiento con los requisitos legales
13.2	Gestión de las mejoras e incidentes en la seguridad de información			15.2	Revisiones de la política de seguridad y de la conformidad técnica
				15.3	Consideraciones sobre la auditoria de sistemas
Total: 11 Cláusulas (numeradas del 5 al 15) y 39 Categorías					

Del mismo modo, mediante Resolución Ministerial N° 129-2012-PCM del 23.MAY.2012, la Presidencia del Consejo de Ministros aprobó el uso obligatorio de la de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de la seguridad de la información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática. Debiendo indicar que dicha Norma Técnica Peruana se basa en el estándar internacional ISO/IEC 27001:2005.

Las principales normas informáticas emitidas por este organismo del estado y que son aplicables al presente trabajo de tesis se encuentran en el **Anexo N° 4**.

1.3. Normativa relacionada a la propia entidad sujeta a control gubernamental

Al momento de realizar auditorías gubernamentales en entidades públicas es importante que el auditor considere dentro de su evaluación la revisión de los diferentes documentos que se detallan a continuación con el fin de tener una idea global de la entidad que se está auditando.

1. **Misión:** Es el motivo, propósito, fin o razón de ser de la existencia de la entidad pública.

2. **Visión:** Es el camino al cual se dirige la entidad pública a largo plazo, el cual sirve para orientar las decisiones estratégicas de dicha entidad.

3. **Organigrama:** Es un esquema gráfico de la estructura organizacional de una entidad pública.

4. **Reglamento de Organización y Funciones (ROF):** Es un documento normativo de gestión institucional en el que se establece la estructura orgánica de la entidad pública así como las funciones generales de cada uno de sus unidades orgánicas.

5. **Manual de Organización y Funciones (MOF):** Es un documento normativo que establece las funciones específicas a nivel de cargo o puesto de trabajo considerando la estructura orgánica y funciones generales establecidas en el Reglamento de Organización y Funciones.

6. **Reglamento Interno de Trabajo (RIT):** Es un documento normativo que establece las obligaciones de trabajo a las que debe sujetarse la entidad pública y sus trabajadores.

7. **Plan Estratégico Institucional (PEI):** Es un instrumento de gestión de mediano plazo (3 a 5 años). En dicho documento se definen entre otros, los objetivos, metas, indicadores y estrategias a seguir por la entidad pública.

8. **Plan Operativo Institucional (POI):** Es un instrumento de gestión de corto plazo (1 año) en el cual se definen las actividades que se llevarán a cabo para el logro de lo consignado en el Plan Estratégico Institucional. En dicho documento se define, entre otros, los objetivos anuales, indicadores, metas, acciones operativas y proyectos.

9. **Plan Estratégico de Tecnologías de Información (PETI):** Es un instrumento de gestión que establece los lineamientos que permitan controlar la adquisición, uso y administración de las tecnologías de información, de tal forma, que contribuyan al logro de los objetivos institucionales de la entidad pública.

10. **Plan Operativo Informático:** Es un instrumento de gestión a corto plazo, que establece las actividades informáticas de las entidades públicas.

11. **Plan Anual de Contrataciones:** Es un documento de gestión que contiene las contrataciones de bienes, servicios y obras que requerirá la entidad pública durante un año.

12. **Políticas Internas:** Son documentos normativos de la entidad pública en la cual se establecen los lineamientos que se aplican dentro de la entidad para llevar a cabo sus actividades.

13. **Procedimientos Internos:** Son documentos normativos de la entidad pública en la cual se establecen las formas de llevar a cabo las actividades dentro de la entidad pública.

14. **Texto Único de Procedimientos Administrativos (TUPA):** Es un documento normativo de cada entidad pública, en el cual se establecen los trámites de los procedimientos administrativos que se realizan ante las distintas dependencias de la entidad (de carácter externo) vinculados con el negocio de la entidad.

15. **Plan de Continuidad:** Es un instrumento de gestión conocido como Plan de Continuidad del Negocio (Business Continuity Plan), el cual tiene como objetivo el mantener la funcionalidad de la organización a un nivel mínimo aceptable durante una eventualidad que puede afectarla (incendio, terremoto u otros). En dicho plan se deben contemplar las medidas preventivas y de recuperación de la entidad.

16. **Plan de Contingencia:** Es un instrumento de gestión aplicado a las áreas de sistemas informáticos. En dicho plan se describe los procedimientos que deben seguir las áreas de sistemas para actuar en caso de una emergencia que interrumpa la operatividad de los sistemas informáticos.

17. **Contrato:** Es el acuerdo vinculante entre dos partes o más exigible por ley, para el suministro, desarrollo, producción, operación o mantenimiento de bienes y/o servicios. En dicho contrato se establece el año o años de garantía de venta, mediante el cual el proveedor se hace responsable de las fallas ocurridas por defectos de fábrica correspondiente a los bienes y/o servicios que se hayan adquirido por parte de la entidad.

18. **Contrato de Mantenimiento Preventivo:** Consiste en la revisión periódica y programada de los bienes y/o servicios adquiridos antes de que se produzca alguna falla. Dicho mantenimiento está amparado por la garantía de venta o por contrato de servicio de mantenimiento post garantía.

19. **Contrato de Mantenimiento Correctivo:** Consiste en la revisión y reparación de los bienes y/o servicios adquiridos ante alguna falla presentada. Dicho mantenimiento está amparado por la garantía de venta o por contrato de servicio de mantenimiento post garantía.

1.4. Marcos de Referencia Internacionales

COSO, ISACA, ISO/IEC son organismos internacionales que proporcionan marcos de referencia internacionales, tales como, Enterprise Risk Management—Integrated Framework, COBIT 4.1 e ISO/IEC 27001:2005 e ISO/IEC 27002:2005 respectivamente, aplicables a las auditorías de sistemas informáticos en entidades del sector público peruano, tal como se detalla a continuación:

1.4.1 Committee of Sponsoring Organizations - COSO

El Comité de Organismos Patronicadores (**CO**mmittee of **S**ponsoring **O**rganizations) es una organización privada "establecida" en los Estados Unidos desde el año 1985, la cual proporciona marcos de trabajo y guías relacionadas a temas de control interno, riesgos empresariales y prevención del fraude; los cuales pueden ser utilizados por las compañías y organizaciones públicas o privadas para evaluar sus propios controles internos para un adecuado Gobierno Corporativo. Dicha organización está conformada por las siguientes instituciones:

- Asociación Americana de Contadores (The American Accounting Association)
- Instituto Americano de Contadores Públicos Certificados (AICPA: The American Institute of CPA's)
- Instituto de Ejecutivos de Finanzas (FEI: The Financial Executives International)
- Asociación de Contadores y Profesionales Financieros en Negocios ((IMA: The Association for Accountants and Financial Professionals in Business)
- Instituto de Auditores Internos (IIA: The Institute of Internal Auditors)

En el año 1992 COSO emitió el documento Marco Integrado de Control Interno (Internal Control - Integrated Framework) el cual establece una definición común de control interno para la evaluación y mejora de los sistemas de control. Dicho documento agrupó en una sola estructura conceptual los distintos enfoques existentes en el ámbito mundial y actualizó los procesos de diseño, implantación y evaluación del control interno. Asimismo, define al control interno como un proceso que constituye un medio para lograr un fin. También señala que es ejecutado por personas en cada nivel de una organización y proporciona seguridad razonable para la consecución de los siguientes objetivos de control interno:

- Eficacia y eficiencia en las operaciones.
- Confiabilidad en la información financiera.
- Cumplimiento de las leyes y regulaciones.

Se indica que el control interno está compuesto por 5 componentes:

1. Ambiente de control
2. Evaluación de riesgos
3. Actividades de control

4. Información y Comunicación
5. Monitoreo (Supervisión)

En el año 2004 COSO emitió el documento Marco Integrado para la Administración de Riesgos Empresariales (Enterprise Risk Management—Integrated Framework) que proporciona un punto de referencia para las organizaciones con el fin evaluar y mejorar sus procesos relacionados a la administración de sus riesgos empresariales (ERM) y proporciona seguridad razonable para la consecución de los siguientes objetivos de control interno:

- Estratégicos.
- Eficacia y eficiencia en las operaciones.
- Confiabilidad en la información financiera.
- Cumplimiento de las leyes y regulaciones.

Asimismo, este enfoque amplía los componentes propuestos en el documento Marco Integrado de Control Interno a 8 componentes:

1. Ambiente interno
2. Establecimiento de objetivos
3. Identificación de eventos
4. Evaluación de riesgos
5. Respuesta a los riesgos
6. Actividades de control
7. Información y comunicación
8. Supervisión

Al respecto, COSO es un marco de referencia internacional que contribuye a identificar controles en todos los niveles de la entidad, el cual incluye controles en las tecnologías de información. Dichos controles en las tecnologías de información constituyen los medios a través de los cuales se puede asegurar que dichas TI son manejados en términos de eficacia, eficiencia y economía en armonía con la normativa vigente.

Es de significar que la 37 Normas de Control Interno, aprobadas mediante Resolución de Contraloría N° 320-2006-GC del 30.OCT.2006, han tomando como antecedente el documento Marco Integrado para la Administración de Riesgos Empresariales emitido por COSO.

1.4.2 Information Systems Audit and Control Association - ISACA

La Asociación de Auditoría y Control de Sistemas de Información - ISACA (**I**nformation **S**ystems **A**udit and **C**ontrol **A**ssociation) es una asociación privada fundada en Estados Unidos en el año 1967 con el fin de contar con una

fuente centralizada de información y guía relacionada a los controles de auditoría en los sistemas computarizados. Al respecto, ISACA ha emitido desde el año 1996 seis versiones[4] relacionadas a los Objetivos de Control para la Información y la Tecnología relacionada – COBIT (**C**ontrol **OB**jetives for **I**nformation and related **T**echnology) con el fin de proporcionar un marco de trabajo para el Gobierno de TI.

Dicho marco de trabajo divide a las TI en 34 procesos (objetivos de control de alto nivel) agrupados en 4 dominios, tal como se muestra a continuación:

- Planificar y Organizar (Planificar): Este dominio considera que las TI tienen que ser planificadas y organizadas, de tal manera, que éstas contribuyan a alcanzar los objetivos de la entidad; es decir proporciona dirección para los dominios "Adquirir e Implantar" y "Entregar y Dar Soporte".

- Adquirir e Implantar (Construir): Con el fin que las TI contribuyan a alcanzar los objetivos de la entidad, éstas deben ser identificadas, desarrolladas o adquirida. Asimismo, este dominio considera las adecuaciones y/o cambios internos de los sistemas ya existentes de la entidad.

- Entregar y Dar Soporte (Ejecutar): Este dominio recibe las TI del dominio "Adquirir e Implantar" con el fin de que utilizables para el usuario final. Está relacionado a la prestación de los servicios de TI, el cual incluye la administración de la seguridad, continuidad, soporte del servicio a los usuarios y de las instalaciones operacionales, de tal forma, que contribuyan a la confidencialidad, integridad y disponibilidad de la información de la entidad.

- Monitorear y Evaluar (Monitorear): Las TI tienen que ser monitoreadas y evaluadas regularmente con el fin de asegurar que éstas cumplan con los fines por las cuales fueron implantadas.

Cuadro de Objetivos de Control de alto nivel - COBIT

DOMINIOS Y PROCESOS							
PLANIFICAR Y ORGANIZAR (Planificar)		**ADQUIRIR E IMPLANTAR (Construir)**		**ENTREGAR Y DAR SOPORTE (Ejecutar)**		**MONITOREAR Y EVALUAR (Monitorear)**	
PO1	Definir el plan estratégico de TI	AI1	Identificar soluciones automatizadas.	DS1	Definir y administrar niveles de servicio.	ME1	Monitorear y evaluar el desempeño de TI.
PO2	Definir la arquitectura de la información	AI2	Adquirir y mantener el software aplicativo.	DS2	Administrar servicios de terceros.	ME2	Monitorear y evaluar el control interno
PO3	Determinar la dirección tecnológica	AI3	Adquirir y mantener la infraestructura tecnológica	DS3	Administrar desempeño y capacidad.	ME3	Garantizar cumplimiento regulatorio.

[4] *Versiones 1, 2, 3, 4, 4.1 y 5 emitidas en los años 1996, 1998, 2000, 2005, 2007 y 2012 respectivamente.*

PO4	Definir procesos, organización y relaciones de TI	AI4	Facilitar la operación y el uso.	DS4	Garantizar la continuidad del servicio.	ME4	Proporcionar gobierno de TI.
PO5	Administrar la inversión en TI	AI5	Adquirir recursos de TI.	DS5	Garantizar la seguridad de los sistemas.		
PO6	Comunicar las aspiraciones y la dirección de la Gerencia	AI6	Administrar cambios.	DS6	Identificar y asignar costos.		
PO7	Administrar recursos humanos de TI	AI7	Instalar y acreditar soluciones y cambios.	DS7	Educar y entrenar a los usuarios.		
PO8	Administrar calidad			DS8	Administrar la mesa de servicio y los incidentes.		
PO9	Evaluar y administrar riesgos de TI			DS9	Administrar la configuración.		
P10	Administrar proyectos			DS10	Administrar los problemas.		
				DS11	Administrar los datos.		
				DS12	Administrar el ambiente físico.		
				DS13	Administrar las operaciones.		
Total: 34 Objetivos de Control							

Fuente: Cobit 4.1

Asimismo los 34 Objetivos de Control se subdividen en 210 objetivos de control específicos, los cuales se encuentran detallados en el **Anexo N° 5** del presente trabajo de tesis.

Al respecto, COBIT clasifica los controles de TI de la siguiente manera:

a. Controles Generales de TI: Son los controles que están diseñados para administrar y monitorear el entorno de tecnologías de información y en consecuencia, afectan a todas las actividades relacionadas con los sistemas de información. Dichos controles son los detallados en los dominios "Planificar y Organizar" y "Monitorear y Evaluar" de las TI.

b. Controles Detallados de TI: Son los controles aplicados a la Adquisición e Implementación así como de la Entrega y Soporte de TI.

1.4.3 La International Organization for Standardization y la International Electrotechnical Commission – ISO /IEC

La Organización Internacional de Normalización (ISO) - International Organization for Standardization, fundada el año 1947 con sede en Ginebra (Suiza), es el organismo encargado de promover el desarrollo de normas

internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Asimismo, la Comisión Electrotécnica Internacional (IEC) - International Electrotechnical Commission es una organización fundada en 1906, que también tiene su sede en Ginebra (Suiza), encargada de la normalización en los campos eléctrico, electrónico y tecnologías relacionadas.

Al respecto, la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) han desarrollado conjuntamente normas ISO/IEC, entre las cuales se encuentran la ISO/IEC 27001:2005 e ISO/IEC 27002:2005, que proporcionan un marco de gestión de la seguridad de la información aplicable para cualquier tipo de organización (pública o privada) sin importar su tamaño (grande o pequeña).

a. ISO/IEC 27001:2005: Indica cómo puede una organización implantar un Sistema de Gestión de la Seguridad de la Información (SGSI) con el fin de medir la efectividad de los controles implementados.

- Proviene del estándar nacional británico BS7799-2:1999 y BS7799-2:2002.
- Publicada el 15.OCT.2005.
- Es certificable a través de auditores externos de entidades independientes.
- En su Anexo A, enumera en forma de resumen los 39 objetivos de control y 133 controles que desarrolla la norma ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. Por tanto, para cumplir este estándar se tiene que cumplir con la norma ISO/IEC 27002:2005.
- En el Perú se le conoce como Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de la seguridad de la información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

b. ISO/IEC 27002:2005: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a la gestión de la seguridad de la información.

- Proviene del estándar nacional británico BS7799-1:1999, estándar internacional ISO/IEC 17799:2000 e ISO/IEC 17799:2005.
- El 01.JUL.2007, el estándar ISO 17799:2005 cambio de nombre a ISO/IEC 27002:2005 manteniendo 2005 como año de edición.
- No es certificable, no se establece un esquema de certificación.

- Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios especificando en forma detallada cómo implementar dichos controles.
- En el Perú se le conoce como Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI Tecnología 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.

Resumen del Capítulo 1

En el presente Capítulo se ha detallado y explicado la normativa que sirve como base para proponer una metodología que permita guiar el proceso de auditorías de sistemas informáticos en el sector público peruano. Entre dicha normativa se encuentra la relacionada al Sistema Nacional de Control Peruano, la cual incluye la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, Reglamento de los Órganos de Control Institucional, Ley de Control Interno de las Entidades del Estado, Normas de Control Interno, Guía para la implementación del Sistema de Control Interno de las entidades del Estado, Normas de Auditoría Gubernamental y Manual de Auditoría Gubernamental.

Asimismo, se consideró normativa emitida por la Presidencia del Consejo de Ministros, entre la cual podemos resaltar las relacionadas al uso obligatorio de las Normas Técnicas Peruanas NTP-ISO/IEC 17799:2007 y NTP-ISO/IEC 27001:2008; referidas a las buenas prácticas para la gestión de la seguridad de la información y sistemas de gestión de la seguridad de la información respectivamente.

Del mismo modo, se hizo mención a normativa utilizada por la propia entidad sujeta a control, entre las cuales, se encuentra la Misión, Visión, Organigrama, Reglamento de Organización y Funciones, Manual de Organización y Funciones, Reglamento Interno de Trabajo, Plan Estratégico Institucional, Plan Operativo Institucional, Plan Estratégico de Tecnologías de Información, Plan Operativo Informático, Plan Anual de Contrataciones, Políticas Internas, Procedimientos Internos, Texto Único de Procedimientos Administrativos, Plan de Continuidad, Plan de Contingencia y Contratos de Mantenimiento Preventivo y Correctivo.

Por último, se consideró los marcos de referencia internacionales COSO-ERM, COBIT 4.1 e ISO/IEC 27001 y 27002 emitidos por las siguientes entidades internacionales COmmittee of Sponsoring Organizations (COSO), Information Systems Audit and Control Association (ISACA) así como la International Organization for Standardization (ISO) e International Electrotechnical Commission (IEC) respectivamente.

Capítulo 2

Propuesta metodológica que permite guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos del Sector Público Peruano

La auditoría gubernamental enfocada a los sistemas informáticos está compuesta por las siguientes tres etapas consecutivas:

- Planificación
- Ejecución y
- Elaboración de Informe de Auditoría.

Cada una de dichas etapas está compuesta por una serie de actividades, las cuales son detalladas en la propuesta metodológica que se muestra a continuación:

METODOLOGÍA DE AUDITORÍA DE SISTEMAS INFORMÁTICOS EN ENTIDADES DEL SISTEMA NACIONAL DE CONTROL

Versión 1.0

INDICE

INTRODUCCIÓN

La presente metodología (versión 1.0) ofrece a los auditores gubernamentales del sector público peruano pertenecientes al Sistema Nacional de Control Peruano un instrumento útil para guiar las auditorías de sistemas informáticos **en entidades públicas**, permitiendo de esta manera, alcanzar los siguientes objetivos:

- Facilitar la comunicación y entendimiento entre los integrantes de la Comisión de Auditoría Gubernamental, teniendo en cuenta sus roles y responsabilidades.
- Indicar los pasos que deben realizar los auditores gubernamentales en las etapas de Planificación, Ejecución y Elaboración del Informe de Auditoría, correspondientes a las auditorías gubernamentales de tipo informático.
- Indicar cuándo utilizar los estándares internacionales tales como COSO, COBIT e ISO/IEC 27002 en las auditorías gubernamentales de tipo informático que permitan la identificación de riesgos asociados a los procesos de la entidad.
- Indicar los diversos documentos que deben ser emitidos en cada una de las etapas de las auditorías gubernamentales de tipo informático.

1. ALCANCE

La presente metodología es aplicable a todas las auditorías gubernamentales de tipo informático que se realicen en entidades públicas a cargo de auditores gubernamentales que pertenezcan al Sistema Nacional de Control Peruano.

2. MARCO CONCEPTUAL

La Metodología de Auditoría de Sistemas Informáticos en entidades del Sistema Nacional de Control Peruano se basa en el marco normativo emitido por la Contraloría General de la República en su calidad de ente rector técnico del Sistema Nacional de Control Peruano.

Asimismo, la presente metodología toma en cuenta la Norma Técnica Peruana (NTP-ISO/IEC 17799:2007) cuyo cumplimiento es obligatorio en las entidades públicas pertenecientes al Sistema Nacional de Informática según lo establecido por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros en su calidad de ente rector técnico del Sistema Nacional de Informática.

Del mismo modo, se hace referencia a los estándares internaciones COSO, COBIT e ISO/IEC 27002.

3. ROLES

Las auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano están conformadas por Comisiones de Auditorías, las cuales están integradas por personal que cumple los siguientes roles:

- **Jefe del Órgano de Control Institucional (OCI):**
  Es la persona que planea, organiza y dirige las auditorías gubernamentales, de conformidad a las disposiciones que regulan el Sistema Nacional de Control y las normas que emita la Contraloría General de la República; con el fin de contribuir con el cumplimiento de los fines y metas institucionales.

- **Supervisor:**
  Es la persona que supervisa las auditorías gubernamentales relacionadas a temas informáticos, de acuerdo a las disposiciones que regulan el Sistema Nacional de Control; con el fin de formular recomendaciones que permitan contribuir con el cumplimiento de los fines y metas institucionales.

  Asimismo, es la persona encargada de verificar el trabajo realizado por el Auditor Encargado y Auditores conformantes de la Comisión de Auditoría.

- **Auditor Encargado:**
  Es la persona que realiza las auditorías gubernamentales relacionadas a temas informáticos, de acuerdo a las disposiciones que regulan el Sistema Nacional de Control; con el fin de formular recomendaciones que permitan contribuir con el cumplimiento de los fines y metas institucionales.

Asimismo, es la persona encargada de guiar, verificar y revisar el trabajo de los Auditores conformantes de la Comisión de Auditoría.

- **Auditores:**
  Es la persona o personas que se encargan de desempeñar el trabajo que el Auditor Encargado les asigne relacionado a las auditorías gubernamentales de temas informáticos, de acuerdo a las disposiciones que regulan el Sistema Nacional de Control; con el fin de formular recomendaciones que permitan contribuir con el cumplimiento de los fines y metas institucionales.

Es importante indicar que cada integrante de la Comisión de Auditoría puede asumir otros roles, dependiendo del alcance y características de la auditoría gubernamental.

4. RESPONSABILIDADES

Cada uno de los integrantes de la Comisión de Auditoría, tienen una serie de responsabilidades a desempeñar durante la auditoría gubernamental en función del rol que cumplan. En ese sentido, las responsabilidades de cada uno de los integrantes de la Comisión de Auditoría son las siguientes:

a. Jefe del Órgano de Control Institucional:

- Planear, organizar y dirigir la auditoría gubernamental respecto de los actos y operaciones de la entidad, sobre la base de los lineamientos y cumplimiento del Plan Anual de Control; a fin de elevar informes de auditoría ante el Titular de la entidad, en los cuales se consignen recomendaciones orientadas a contribuir con el logro de los fines y metas institucionales.
- Planear, organizar y dirigir la ejecución auditorías gubernamentales que disponga la Contraloría General, así como, las que sean requeridas por el Titular de la entidad, con opinión previa favorable del Órgano Superior de Control; a fin de procurar alcanzar los objetivos propuestos y emitir las recomendaciones que correspondan.
- Aprobar y remitir los Informes de Auditoría Gubernamental a la Contraloría General, así como al Titular de la entidad; a fin de poner en conocimiento el resultado de las mismas, y se adopten las medidas correctivas pertinentes.
- Formular, ejecutar y evaluar el Plan Anual de Control, a fin de dar cumplimiento a los lineamientos y disposiciones emitidas por la Contraloría General.
- Planear, organizar y dirigir el seguimiento de implementación de recomendaciones producto de las auditorías realizadas, verificando su implementación efectiva, a fin de contribuir con la superación de las situaciones identificadas.
- Aprobar el Plan y Programa de Trabajo de Auditoría.

b. Responsabilidades del Supervisor:

- Supervisar cada una de las fases de la auditoría gubernamental (planeamiento, ejecución y elaboración del informe de auditoría) a fin de asegurar el cumplimiento de las normas que lo regulan.
- Revisar y aprobar los procedimientos de auditoría gubernamental establecidos en el Plan y Programa de Trabajo de la Auditoría, antes del inicio del trabajo de campo.
- Programar el personal profesional que participará de la auditoría gubernamental.
- Vigilar el progreso de la auditoría gubernamental, lo cual incluye el tiempo y costos de la auditoría.
- Solucionar los problemas identificados por el Auditor Encargado y Auditores conformantes de la Comisión de Auditoría.
- Supervisar y asesorar al Auditor Encargado, así como orientar a otros miembros conformantes de la Comisión de Auditoría.
- Supervisar la elaboración del Informe de Auditoría Gubernamental.
- Revisar los papeles de trabajo de la Auditoría Gubernamental.

c. Responsabilidades del Auditor Encargado:

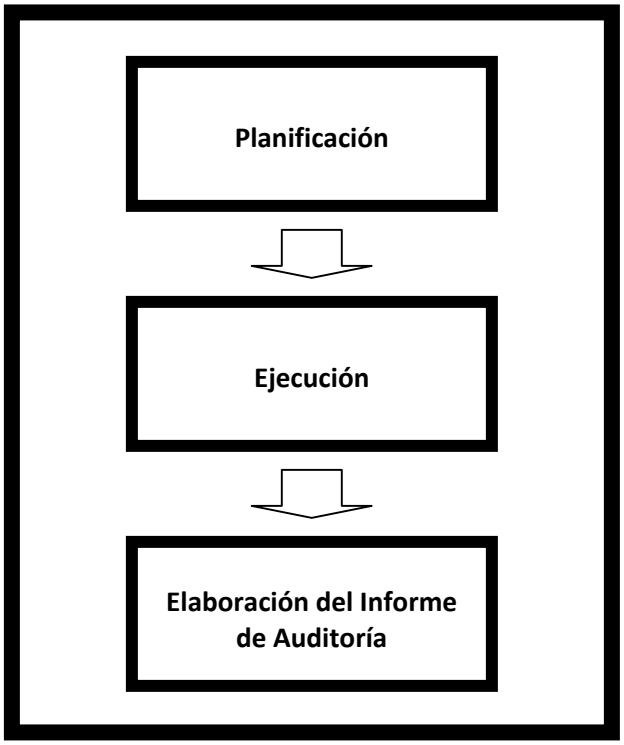
- Realizar cada una de las fases de la auditoría gubernamental (planeamiento, ejecución y elaboración del informe de auditoría) con el propósito de verificar selectivamente los sistemas informáticos con el objetivo de plantear recomendaciones que contribuyan a la administración y gestión de la entidad auditada.
- Identificar los problemas de auditoría para coordinarlos con el Supervisor.
- Asesorar y asistir a los auditores de la Comisión de Auditoría con el fin que se comprendan los objetivos de la auditoría.
- Revisar los papeles de trabajo que preparen los auditores de la Comisión de Auditoría, evaluando la evidencia obtenida.

d. Responsabilidades de los Auditores:

- Comprender y ejecutar los procedimientos de auditoría asignados.
- Informar al Auditor Encargado sobre asuntos o problemas que se detecten.
- Elaborar los papeles de trabajo.

5. ETAPAS DE LA AUDITORÍA GUBERNAMENTAL

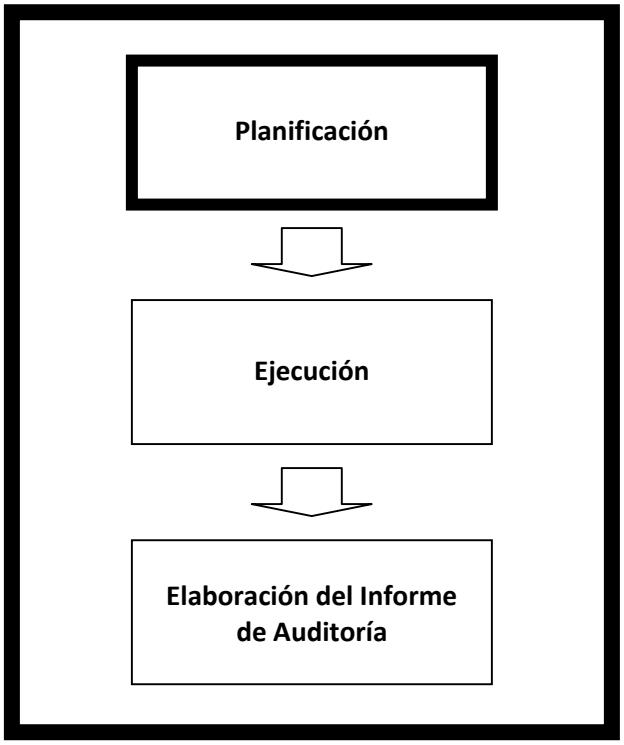
Las auditorías de sistemas informáticos en entidades del Sistema Nacional de Control Peruano, está compuesta por tres etapas consecutivas: Planificación, Ejecución y Elaboración del Informe de Auditoría, tal como se muestra a continuación:



5.1 ETAPA DE PLANIFICACIÓN

La etapa de Planificación representa la primera etapa de la auditoría gubernamental de sistemas informáticos, tal como, se muestra en el siguiente gráfico:

Etapas de la Auditoría Gubernamental



5.1.1 OBJETIVO

Establecer las diversas actividades que permitan guiar la planificación de las auditorías gubernamentales enfocadas a los sistemas informáticos.

5.1.2 ACTIVIDADES QUE INCLUYEN LA PRESENTE ETAPA

a. SE INICIA CON: Planificación General de la auditoría gubernamental.

1. El objetivo del Planeamiento General es planificar todas las auditorías que serán realizadas por las entidades pertenecientes al Sistema Nacional de Control, en el periodo de un año, utilizando criterios de materialidad, economía, objetividad y oportunidad. **(NAGU 2.10: PLANIFICACIÓN GENERAL)**

Para poder realizar dicha planificación, la Contraloría General de la República define los lineamientos (disposiciones técnicas) a seguir

para la elaboración del Plan Anual de Control, el cual es realizado por el Órgano de Control Institucional de cada entidad pública, las cuales están dirigidas a contribuir al logro de los objetivos y metas institucionales.

Al respecto, para determinar las auditorías a realizar se prioriza, entre otros, los siguientes temas:

- Riesgos identificados.
- Denuncias realizadas.
- Monto económico involucrado.
- Falta de controles internos.
- Áreas o procesos de importancia.
- Indicios de irregularidades detectadas.
- Conocimiento que el órgano de control institucional posee de la entidad.

Cabe indicar que en el Plan Anual de Control están incluidas las auditorias gubernamentales enfocadas a los sistemas informáticos.

2. En ese sentido, el Jefe del Órgano de Control Institucional se reunirá con el personal a su cargo, para programar las auditorías a considerarse en el Proyecto del Plan Anual de Control, en concordancia con los lineamientos de la Contraloría General de la República, considerando el orden y tiempo de su ejecución.

Luego, el Jefe del Órgano de Control Institucional procederá a la revisión y visación del Plan Anual de Control, para que sea elevado al Titular de la entidad con el fin de que se comprometa a asignar al Órgano de Control Institucional los recursos necesarios para la ejecución de las auditorías.

3. Posteriormente, el Jefe del Órgano de Control Institucional remitirá el Proyecto del Plan Anual de Control a la Contraloría General de la República para su evaluación. De existir alguna observación al Proyecto del Plan Anual de Control, la Contraloría General notificará al Órgano de Control Institucional para la subsanación correspondiente.

Finalmente, la Contraloría General de la República procede a su aprobación mediante Resolución de Contraloría, la cual es publicada en el diario Oficial El Peruano.

b. CONTINÚA CON: Planificación Específica de la Auditoría.

4. El objetivo de la Planificación Específica es determinar la estrategia que será utilizada en la ejecución de la auditoría de sistemas informáticos, el cual incluye el planeamiento y programa de auditoría. **(NAGU 2.20: PLANEAMIENTO DE LA AUDITORÍA)**

5. Una vez aprobada la auditoría gubernamental (programada o no programada), el Jefe del Órgano de Control Institucional designa al Supervisor y Auditor Encargado de la auditoría gubernamental.

6. El Supervisor en coordinación con el Auditor Encargado proceden a revisar, evaluar y actualizar la información que contiene el archivo permanente **(NAGU 2.40: ARCHIVO PERMANENTE)**, el cual incluye comprender y tomar conocimiento inicial de las operaciones de la entidad auditada considerando, entre otros, los siguientes:

- Leyes y reglamentos aplicables a la entidad.
- Misión, Visión y Organigrama de la entidad.
- Plan Estratégico Institucional (PEI) y Plan Operativo Institucional (POI).
- Plan Estratégico de Tecnologías de Información (PETI) y Plan Operativo Informático.
- Plan Anual de Contrataciones.
- Reglamento de Organización y Funciones (ROF), Manual de Organización y Funciones (MOF) y Reglamento Interno de Trabajo (RIT).
- Políticas Internas.
- Procedimientos Internos.
- Texto Único de Procedimientos Administrativos (TUPA).
- Planes de Continuidad.
- Planes de Contingencia.
- Contratos de Mantenimiento Preventivo - Correctivo relacionados a las tecnologías de información utilizadas por la entidad.

7. Asimismo, se debe revisar documentación de auditorías anteriores relacionadas a temas informáticos, realizadas por el Órgano de Control Institucional, Contraloría General de la República ó Sociedades de Auditorías (SOA). En dicha revisión, se debe considerar las recomendaciones emitidas por dichos informes que estén relacionados a los temas que se van a evaluar.

8. Luego, se debe proceder a tomar conocimiento de los temas relacionados a las tecnologías de información, los cuales dan soporte a la misión de la entidad, entre los cuales se tienen:

- Lugares físicos:
  - Instalaciones
  - Centros de Cómputo (data center)

- Hardware
  - Microcomputadores, Servidores

- Software
  - Sistemas operativos
  - Lenguajes de programación
  - Sistemas de información realizados por la propia entidad así como los adquiridos a proveedores externos
  - Licencias de software
  - Base de datos

- Telecomunicaciones
  - Redes (LAN, WAN)
  - Internet
  - Intranet
  - Extranet

- Documentación
  - Normas, estándares, políticas, y procedimientos
  - Manuales del sistema
  - Manuales del usuario
  - Flujogramas de procesos más importantes

- Personal
  - Personal que trabaja en las áreas de TI y servicios prestados por terceros
  - Principales usuarios de cada sistema
  - Satisfacción de los usuarios finales

- Presupuesto asignado a las TI

9. Como siguiente paso, se procede a reunir información preliminar sobre los controles y riesgos de la entidad mediante requerimientos de información, entrevistas, encuestas, revisión de documentos y/o visitas. La información obtenida mediante estos métodos, se convierte en la base para identificar y documentar la importancia de cada control y riesgo. Por ello, es importante identificar situaciones de riesgo asociados a cualquier debilidad de los controles que se hayan implementado en la entidad.

Sobre el particular, la identificación preliminar de controles y riesgos ayudan a definir las áreas críticas de tecnologías de información así como las áreas de la entidad, procesos de TI y temas de interés a ser examinados, es decir, cómo hacerlo y si resulta conveniente hacerlo; efectuándose un primer análisis de la problemática a ser evaluada, con el fin de poder establecer el objetivo general y objetivos específicos de la auditoría. En ese sentido, las 32 normas de control interno que conforman los 5 componentes del Sistema Control Interno (el cual está basado en el marco internacional COSO) contribuyen a la identificación preliminar de dichos controles y riesgos. **(Ver Anexo A-1)**

10. Una vez concluido el punto anterior, el Supervisor y el Auditor Encargado proceden a preparar el documento "Plan y Programa de Auditoría" **(NAGU 2.30: PROGRAMAS DE AUDITORÍA)**, el cual incluye los siguientes puntos:

	Rubro	Detalle
1	Nombre de la Auditoría	Se consigna el nombre de la auditoría gubernamental que se está realizando.
2	Origen	Es el motivo o razón por la cual se está realizando la auditoría gubernamental.
3	Objetivos	
	a. Objetivo General	Es lo que se desea lograr en términos globales, como resultado de la auditoría gubernamental.
	b. Objetivos Específicos	Describen lo que se desea lograr en términos concretos para alcanzar el objetivo general.
4	Naturaleza	Se específica el tipo de auditoría.
5	Alcance	Área(s) que se auditarán así como el periodo de tiempo que se va a auditar.
6	Criterios de Auditoría	Son parámetros que se toman en cuenta al momento de realizar la auditoría; es decir, normatividad que permita comparar condiciones existentes.
7	Procedimientos Mínimos a Ejecutar	Son las actividades que se realizarán durante el trabajo de campo de la auditoría gubernamental con el fin de alcanzar los objetivos trazados.
8	Personal asignado	Se incluyen los nombres de cada uno de los integrantes de la Comisión de Auditoría, especificando el cargo que ocupan en la Comisión así como sus profesiones.
9	Presupuesto de tiempo	Se consigna las fechas del inicio y fin de la auditoría gubernamental, especificando las fechas para cada una de sus fases que son: – Planificación – Ejecución – Elaboración de Informe de Auditoría
10	Fecha de Elaboración	Se consigna la fecha de emisión.
11	Firma	Incluye firma del Auditor Encargado Supervisor y Jefe del OCI.

11. El Jefe del Órgano de Control Institucional procede a aprobar y firmar el “Plan y Programa de Auditoría”, el cual previamente fue firmado por el Auditor Encargado y Supervisor.

12. Se procede a armar los papeles de trabajo de la etapa de Planificación.

c. FINALIZA CON: Aprobación del “Plan y Programa de Auditoría” por parte del Jefe del Órgano de Control Institucional.

5.1.3 ENTREGABLES

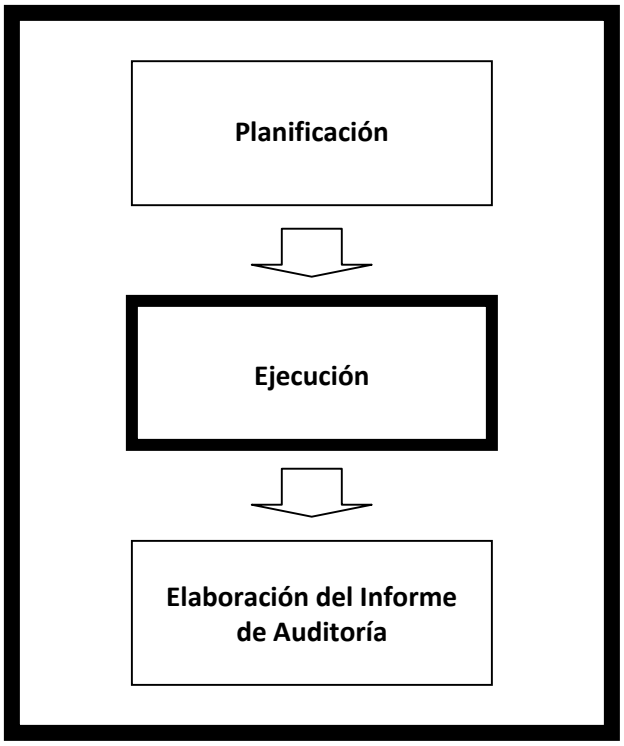
La etapa de Planificación de las auditorías gubernamentales enfocada a los sistemas informáticos tiene como entregables los siguientes documentos:

- Plan Anual de Control
- Actualización de Archivo Permanente
- Plan y Programa de Auditoría
- Papeles de Trabajo de la etapa de Planificación

5.2 ETAPA DE EJECUCIÓN

La etapa de Ejecución representa la segunda etapa de la auditoría gubernamental de sistemas informáticos, tal como, se muestra en el siguiente gráfico:

Etapas de la Auditoría Gubernamental



5.2.1 OBJETIVO

Establecer las diversas actividades que se realizan durante el trabajo de campo de las auditorías gubernamentales enfocadas a los sistemas informáticos.

5.2.2 ACTIVIDADES QUE INCLUYE LA PRESENTE ETAPA

a. SE INICIA CON: Memorándum de Presentación de la Comisión de Auditoría.

1. Mediante Memorándum de Presentación de la Comisión de Auditoría, el Jefe del Órgano de Control Institucional comunica al Jefe del área auditada el inicio de la auditoría gubernamental, en el que se consigna el nombre de la auditoría y los nombres del Supervisor y Auditor Encargado de la Comisión de Auditoría con el fin de que se disponga

que sus unidades organizacionales dependientes brinden las facilidades del caso en la entrega oportuna de la información y documentación sustentatoria.

b. CONTINÚA CON:

2. El Supervisor y Auditor Encargado de la Comisión de Auditoría se reunirán con los auditores integrantes de la Comisión, a fin de comunicar y explicar el Plan y Programa de Auditoría. Asimismo, el Auditor Encargado asigna a cada uno de los Auditores integrantes las tareas y procedimientos mínimos a realizar.

3. El Supervisor, Auditor Encargado y Auditores se entrevistarán con el Jefe del área auditada o a quién éste delegue, con el fin de coordinar las reuniones de trabajo y los requerimientos de información que se efectuarán con el personal dependiente de su área. De esta manera, se busca un entendimiento general del proceso que se está auditando (módulos y/o herramientas asociadas a las mismas), identificando los sistemas de información que soportan determinadas actividades clave. Asimismo, a través de flujogramas se diagrama el proceso que se está auditando, los cuales deben ser validados por el área auditada.

De manera complementaria al entendimiento de los procesos que se están auditando y con la finalidad de confirmar el entendimiento del proceso, se validan los flujogramas a través de la ejecución de pruebas de recorrido.

Estas pruebas de recorrido consideran la selección de uno o varios casos representativos de cada flujograma y se solicitan las evidencias y sustentos apropiados para cada prueba con el fin de verificar que se cumplan las actividades y controles asociados al proceso, así como identificar posibles puntos débiles de control y de mejora; siguiendo la siguiente estructura:

Pruebas de Recorrido del Diagrama de Flujograma del Proceso que se está auditando						
N°	Fecha	Pruebas (Adjuntar evidencias que sustenten las pruebas realizadas)	Actividades realizadas	Participantes de la entidad	Participantes de la Comisión de Auditoría	Resultados (Hallazgos y/o comentarios de las pruebas realizadas)

4. El Auditor Encargado en coordinación con los Auditores de la Comisión de Auditoría procederán a la evaluación de la estructura de control interno de las Tecnologías de Información (TI) relacionadas a los sistemas informáticos de la entidad que se está auditando **(NAGU 3.10: EVALUACIÓN DE LA ESTRUCTURA DEL CONTROL INTERNO)** para la identificación de controles de TI relacionados a:

- Identificar el nivel de desarrollo, organización y vigencia del sistema de control interno de TI.
- Identificar los elementos de control que conforman el sistema de control interno de TI.
- Identificar las deficiencias y vacíos que presenta el sistema de control interno de TI.
- Identificar los principales procesos y áreas críticas de TI que requieren un examen profundo.

Al respecto, se debe proceder a comprobar que los controles de TI estén funcionando correctamente, lo cual incluye realizar el análisis de brechas de los controles de seguridad de la información relacionado al proceso o procesos que se están auditando.

Sobre el particular, el Auditor Encargado así como los Auditores pueden utilizar los estándares internacionales COBIT e ISO/IEC 27002 para la evaluación y revisión correspondiente de los controles de TI, tal como se muestra a continuación:

Cuadro Comparativo COBIT – ISO/IEC 27002

<table>
<tr><th></th><th>COBIT</th><th>ISO/IEC 27002:2005
(NTP-ISO/IEC 17799:2007)</th></tr>
<tr><td rowspan="2">Controles Generales de TI</td><td>Planificación y Organización</td><td rowspan="4">5. Política de Seguridad
6. Aspectos organizativos para la seguridad
7. Clasificación y control de activos
8. Seguridad en recursos humanos
9. Seguridad física y del entorno
10. Gestión de comunicaciones y operaciones
11. Control de accesos
12. Adquisición, desarrollo y mantenimiento de sistemas
13. Gestión de incidentes en la seguridad de información
14. Gestión de continuidad del negocio
15. Cumplimiento</td></tr>
<tr><td>Monitoreo</td></tr>
<tr><td rowspan="2">Controles Detallados de TI</td><td>Adquirir e Implementar</td></tr>
<tr><td>Entrega y Soporte</td></tr>
</table>

Es de significar que en los **Anexos N° A-2 y A-3,** se puede apreciar cómo están alineados los controles COBIT e ISO/IEC 27002:2005 y viceversa respectivamente.

A continuación, se presentan los resultados obtenidos:

Brecha de controles de seguridad de la información					
N°	Fecha	Proceso de la entidad sujeto a evaluación	Dominio evaluado	Control Evaluado	Situación identificada

Asimismo, en el caso que la comprobación de los controles internos de los procesos de TI muestre que los controles generales de TI son satisfactorios, la Comisión de Auditoría debe considerar la posibilidad de reducir el nivel de pruebas planificado para los controles detallados, dado que la evidencia de auditoría de los controles generales de TI eficaces contribuirá a garantizar la eficacia de los controles detallados.

Por el contrario, si se comprueba que los controles generales de TI no son satisfactorios, la Comisión de Auditoría debe llevar a cabo pruebas suficientes de los controles detallados, a fin de suministrar evidencia de auditoría que corrobore que éstos están operando con eficacia pese a las deficiencias de los controles generales de TI.

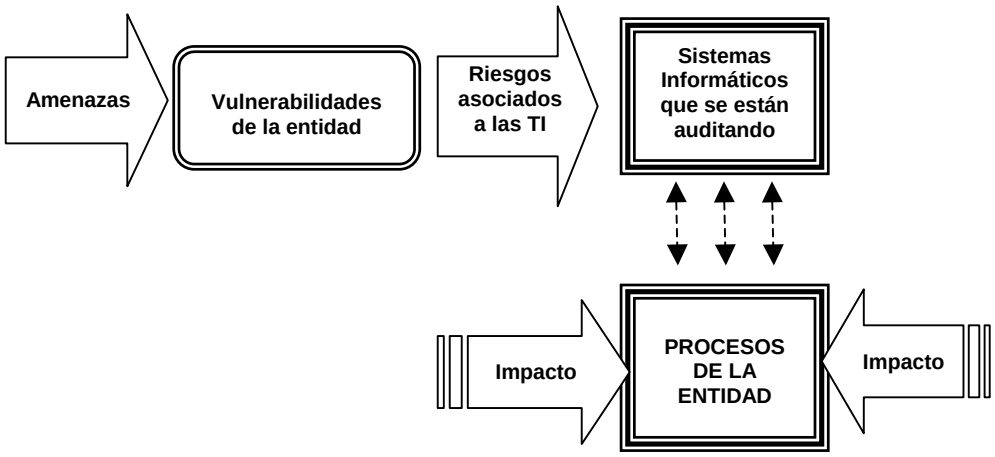
5. Paralelamente, con la información que se viene obteniendo de la evaluación de la estructura de control interno de TI se procede a la **Evaluación de los Riesgos de TI** relacionados a los sistemas informáticos de la entidad que se está auditando. Cabe indicar que los sistemas informáticos están asociados a procesos propios de la entidad. Al respecto, se procede a su evaluación desde el punto de vista de la confidencialidad, integridad y disponibilidad de la información que procesan los sistemas informáticos:

Propiedades de la Información		
Confidencialidad	La información de la entidad debe ser accesada sólo por personal ó procesos autorizados.	Un inadecuado control de la confidencialidad, integridad y disponibilidad de la información puede provocar para la entidad, entre otros, las siguientes consecuencias: - Pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de
Integridad	La información de la entidad debe ser modificada y/o eliminada por personal o procesos autorizados, con el fin de mantener la exactitud y consistencia de su información.	

Disponibilidad	La información de la entidad debe estar disponible en el momento que las personas ó procesos de la entidad lo requieran	confianza. - Interrupción del servicio. - Incumplimiento de metas. - Incumplimiento de acuerdos de servicio - Sanciones, etc.

La evaluación de los riesgos de TI incluye la identificación, valoración (según su probabilidad e impacto) y tratamiento de los riesgos (a través de recomendaciones que son incluidas en el informe de auditoría), tal como se detalla a continuación:

5.1 Identificación de Riesgos de TI: Consiste en identificar los riesgos de TI relacionados a los sistemas informáticos del proceso que se está auditando. Los medios para poder identificarlos son, entre otros, los cuestionarios, encuestas y entrevistas. Al respecto, dichos medios deben estar dirigidas a conocer las funciones del área que se está auditando y cómo dichas funciones se alinean con los objetivos de la entidad con el fin de identificar los eventos que constituyen riesgos de TI, considerando el siguiente gráfico:



Donde:

Amenazas: Son aquellas causales internas ó externas a la entidad que pueden ocasionar consecuencias negativas en la operatividad de la entidad pudiendo ser accidentales o intencionales. Dichas causales pueden ser: personas, materiales, instalaciones y entorno.

Vulnerabilidades: Son debilidades o ausencias de control que facilitan que las amenazas se materialicen. Es de significar que por

sí solas las vulnerabilidades no causan daños. Por lo que sí no son debidamente administradas permitirá que las amenazas se concreten.

Riesgo: Es la probabilidad de que una amenaza pueda activar una vulnerabilidad en particular, afectando los sistemas informáticos de la entidad.

Ejemplo:

Amenaza (Causa)	**Vulnerabilidad** (Debilidades o ausencias de control)	**Riesgo de TI** (Efecto)
Virus informáticos que son transmitidos por medios informáticos	La entidad no actualiza el antivirus en los computadores	Probabilidad es que el virus infecté los computadores
Requerimiento de TI no solicitado por el área usuaria	Infraestructura de TI insuficiente	Probabilidad de que la áreas que utilizan las TI no puedan alcanzar sus objetivos

Cabe indicar que las TI que administren o procesen datos sensibles así como de aquellas que requieren de un gran presupuesto son particularmente vulnerables a la ocurrencia de actos irregulares.

5.2 Valoración de Riesgos de TI: La valoración de los riesgos de TI se efectuará en base a la información obtenida en la "Identificación de riesgos de TI". La evaluación de los riesgos de TI se realizará desde el punto de vista de su probabilidad de ocurrencia así como de su impacto (consecuencias de la materialización del riesgo), permitiendo de esta manera obtener información que permita determinar el nivel de riesgo y las acciones que puedan implementarse (recomendaciones).

Por cada riesgo de TI identificado se evalúan los niveles de probabilidad e impacto considerando las siguientes escalas Cualitativa y Cuantitativa:

Escala Cualitativa de Probabilidad e Impacto

De Probabilidad

Categoría	**Definición**
Probable	Es muy frecuente la materialización del riesgo o se presume que llegará a materializarse.
Posible	Es frecuente la materialización del riesgo o se presume que posiblemente se podrá materializar.
Improbable	Es poco frecuente la materialización del riesgo o se presume que no llegará a materializarse.

De Impacto

Categoría	Definición
Desastroso	Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.
Moderado	Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.
Leve	Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

Fuente: Guía para la implementación del Sistema de Control Interno

Escala Cuantitativa de Probabilidad e Impacto

De Probabilidad

Probabilidad de ocurrencia	Nivel
0 – 25	Improbable
26 – 70	Posible
71 – 100	Probable

De Impacto

Impacto	Nivel
0 – 25	Leve
26 – 70	Moderado
71 – 100	Desastroso

Fuente: Guía para la implementación del Sistema de Control Interno

A través de la matriz de probabilidad e impacto los riesgos pueden ser priorizados. Dicha matriz especifica combinaciones de probabilidad e impacto para calificar a los riesgos como aceptable, tolerable, moderado, importante e inaceptable, tal como se muestra a continuación:

Matriz de probabilidad e impacto

			Impacto		
			1	2	3
			Leve	Moderado	Desastroso
Probabilidad	Probable	3	3: Riesgo Moderado	6: Riesgo Importante	9: Riesgo Inaceptable
	Posible	2	2: Riesgo Tolerable	4: Riesgo Moderado	6: Riesgo Importante
	Improbable	1	1: Riesgo Aceptable	2: Riesgo Tolerable	3: Riesgo Moderado

Fuente: Guía para la implementación del Sistema de Control Interno

La puntuación del riesgo ayuda a guiar las respuestas a los riesgos:

Nivel de Riesgo	**Descripción**
Riesgo Inaceptable	Se requiere acción inmediata. Planes de tratamiento requeridos, implementados y reportados a la Alta Dirección.
Riesgo Importante	Se requiere atención de la alta dirección. Planes de tratamiento requeridos, implementados y reportados a los jefes de las oficinas, divisiones, entre otros.
Riesgo Moderado	Debe ser administrado con procedimientos normales de control.
Riesgo Tolerable	Menores efectos que pueden ser fácilmente remediados. Se administra con procedimientos rutinarios
Riesgo Aceptable	Riesgo insignificante. No se requiere ninguna acción.

Fuente: Guía para la implementación del Sistema de Control Interno

Sobre el particular, es necesario que por cada riesgo se evalúen las medidas de control que la entidad está aplicando con el fin de reducirlos o mantenerlos bajo control y en función a ello se determinen las recomendaciones correspondientes, las cuales son plasmadas en el Informe Final de Auditoría.

De esta manera la entidad podrá tomar las acciones necesarias respecto de los riesgos de TI identificados (evitando, reduciendo, compartiendo, transfiriendo o asumiendo el riesgo).

En consecuencia, a partir de la evaluación de riesgos realizada se pueden recomendar controles que puedan mitigar los riesgos identificados en la entidad que se está auditando.

Ejemplo:

Amenaza (Causa)	**Vulnerabilidad** (Debilidades o ausencias de control)	**Riesgo de TI** (Efecto)	**Recomendación**
Virus informáticos que son transmitidos por medios informáticos	La entidad no actualiza el antivirus en los computadores	Probabilidad es que el virus infecté los computadores	Disponer la actualización periódica de los antivirus de los computadores de la entidad
Requerimiento de TI no solicitado por el área usuaria	Infraestructura de TI insuficiente	Probabilidad de que la áreas que utilizan las TI no puedan alcanzar sus objetivos	Solicitar al área usuaria, los requerimientos de TI necesarios para el cumplimiento de sus funciones

6. Al término de esta evaluación la Comisión de Auditoría emitirá, de ser el caso, el documento Memorándum de Control Interno, en el cual se especifican las debilidades de control interno detectadas. El Memorándum de Control Interno debe ser remitido al Titular de la entidad para la implementación de recomendaciones contenidas en dicho documento, según siguiente detalle:

<table>
<tr><th></th><th>Rubro</th><th>Detalle</th></tr>
<tr><td></td><td>Titulo</td><td>Se especifica: “Memorándum de Control Interno” correspondiente al nombre de la auditoría de sistemas informáticos que se está realizando.</td></tr>
<tr><td>I</td><td>Introducción</td><td>Se deja constancia que los hechos informados no revelan necesariamente todas las debilidades del sistema de control interno realizado a la entidad que se está evaluando, toda vez que la muestra es de carácter selectivo.</td></tr>
<tr><td>II</td><td>Debilidades de Control Interno</td><td rowspan="6">En función a las debilidades de control interno identificadas relacionadas a las 37 normas de control interno (correspondientes a los 5 componentes de la estructura de control Interno), se detallan las principales debilidades de control detectadas en los procesos de sistemas informáticos que se están auditando.</td></tr>
<tr><td></td><td>a. Ambiente de Control</td></tr>
<tr><td></td><td>b. Evaluación del Riesgo</td></tr>
<tr><td></td><td>c. Actividades de Control Gerencial</td></tr>
<tr><td></td><td>d. Información y Comunicación</td></tr>
<tr><td></td><td>e. Supervisión</td></tr>
<tr><td>III</td><td>Conclusiones</td><td>En función a las debilidades de control interno se señalarán las respectivas conclusiones.</td></tr>
<tr><td>IV</td><td>Recomendaciones</td><td>En función de las conclusiones identificadas se establecerán las respectivas recomendaciones.</td></tr>
<tr><td></td><td>Anexos</td><td></td></tr>
</table>

7. Paralelamente, se debe proceder a la Evaluación del cumplimiento de disposiciones legales y reglamentarias **(NAGU 3.20: EVALUACIÓN DEL CUMPLIMIENTO DE DISPOSICIONES LEGALES Y REGLAMENTARIAS)**. Dicha evaluación consiste en:

- Verificar el cumplimiento de la normativa interna y externa aplicable a los sistemas informáticos del proceso que se está auditando, el cual incluye:

Normativa	
Interna	Políticas, Resoluciones, Directivas, Procedimientos, etc.
Externa	Leyes, Reglamentos, Decretos Legislativos, etc. (emitidos por otras entidades públicas aplicables a la entidad que se está auditando)

Para establecer el nivel de cumplimiento, se establece la siguiente tabla:

Nivel de cumplimiento	**Comentario**
No Cumple	Ningún aspecto contenido en la normativa evaluada se cumple.
Cumple Parcialmente	Algunos de los aspectos contenidos en la normativa evaluada se cumplen.
Cumple	Todos los aspectos contenidos en la normativa evaluada se cumplen.

De la verificación realizada y en base al cumplimiento de la normativa interna y externa aplicable a la entidad vinculados al tema que se está auditando, se obtiene el nivel de cumplimiento de la normativa evaluada, según siguiente cuadro:

Normativa evaluada	**Objetivo de la Norma**	**Aspectos contenidos**	**Nivel de cumplimiento**	**Opinión del auditor**

Asimismo, en base a la evaluación de la normativa evaluada, se procede a asociar dicha normativa con las amenazas, vulnerabilidades y riesgos de TI identificados, tal como se muestra a continuación:

Ejemplo:

Amenaza < Causa >	**Vulnerabilidad** (Debilidades o ausencias de control) < Condición >	**Riesgo de TI** < Efecto >	**Normatividad < Criterio >**
Virus informáticos que son transmitidos por medios informáticos	La entidad no actualiza el antivirus en los computadores	Probabilidad es que el virus infecté los computadores	**El Procedimiento interno relacionado a la prevención, detección y eliminación de virus informáticos establece las acciones preventivas que deben realizar los usuarios respecto de los virus informáticos.**
Requerimiento de TI no solicitado por el área usuaria	Infraestructura de TI insuficiente	Probabilidad de que la áreas que utilizan las TI no puedan alcanzar sus objetivos	**Mediante Dec.Leg. N° 1017 se aprobó la Ley de Contrataciones del Estado, el cual establece en su Art.13 las características técnicas de los bienes, servicios y obras a contratar.**

8. Durante la ejecución de la auditoría, el Supervisor se presentará a la Comisión de Auditoría una vez por semana y cada vez que sea requerido, a efecto de evaluar el avance del trabajo de campo, revisando los papeles de trabajo y orientando a la Comisión para el cumplimiento de los objetivos del Plan y Programa de Auditoría. **(NAGU 3.30: SUPERVISIÓN DEL TRABAJO DE AUDITORÍA)**

9. Cada integrante de la Comisión de Auditoría, de acuerdo al avance del trabajo de campo, reunirá evidencia suficiente, competente y relevante sustentada en los respectivos papeles de trabajo, indicando su nombre, fecha de emisión y fuente de origen, los cuales cada dos días serán revisados por el Auditor Encargado, con el fin de verificar si se viene cumpliendo con los objetivos trazados. **(NAGU 3.40: EVIDENCIA SUFICIENTE, COMPETENTE Y RELEVANTE y NAGU 3.50: PAPELES DE TRABAJO)**

10. Los auditores integrantes de la Comisión de Auditoría, elaborarán los documentos de "Aspectos de Importancia" y/o "Comunicación de Hallazgos" que se hayan identificado producto del trabajo de campo realizado, los mismos que serán de conocimiento del Auditor Encargado y del Supervisor. Cabe indicar que los Hallazgos son presuntas deficiencias o irregularidades identificadas como resultado de la aplicación de los procedimientos de auditoría (considerando su materialidad y/o importancia relativa); mientras que los "Aspectos de Importancia" son otras debilidades de control de significación o importancia que han sido identificados en los procesos de TI de la entidad auditada.

Al respecto, los documentos de "Comunicación de Hallazgos" deben cumplir con los siguientes requisitos para ser un Hallazgo de Auditoría, tal como se detalla a continuación:

Requisitos para ser un Hallazgo de Auditoría	
Condición	Situación o hecho detectado.
Criterio	Norma, disposición o parámetro de medición transgredido.
Causa	Razón que motivo el hecho o incumplimiento establecido (cuando haya podido ser identificada a la fecha de comunicación de hallazgos)
Efecto	Resultado adverso o riesgo potencial identificado.

Sobre el particular, si los documentos elaborados por los auditores cumplen con los requisitos para ser un Hallazgo, el Auditor Encargado comunicará por escrito los Hallazgos a los auditados, determinando el plazo en que efectuarán sus aclaraciones o comentarios. En casos especiales, el Auditor Encargado ampliará los plazos otorgados, de acuerdo al requerimiento realizado. **(NAGU 3.60: COMUNICACIÓN DE HALLAZGOS)**

Una vez proporcionadas las aclaraciones o comentarios de la "Comunicación de Hallazgos", los Auditores y Auditor Encargado procederán a su evaluación, consignando los mismos en los papeles de trabajo.

11. El Auditor Encargado remite al Titular y/o nivel Jefatural (al cual se ha estado auditando) el proyecto sugerido de “Carta de Representación” para que en cumplimiento de las Normas de Auditoría Gubernamental procedan a confirmar al Auditor Encargado si han puesto a disposición de la Comisión de Auditoría toda la información importante y necesaria que obra en sus archivos y de ser el caso si han informado de situaciones irregulares que involucren a sus trabajadores; con el fin que no se haya afectado los resultados de la evaluación de la Comisión de Auditoría. **(NAGU 3.70: CARTA DE REPRESENTACIÓN)**

c. FINALIZA CON: Entrega formal del trabajo realizado por lo auditores al Auditor Encargado de la Comisión de Auditoría relacionado a los “Aspectos de Importancia” y/o “Comunicación de Hallazgos” de Auditoría.

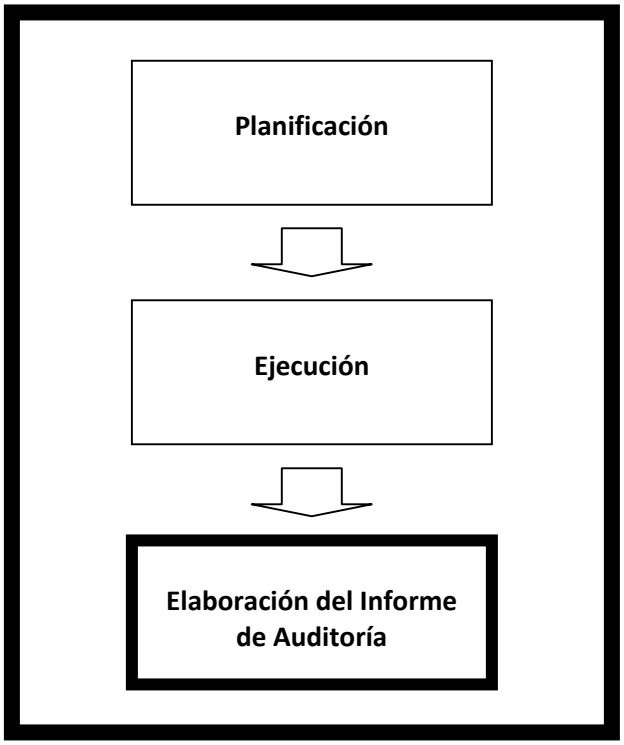
5.2.3 ENTREGABLES

- Memorándum de Control Interno (Si es que se emitió durante la etapa de Ejecución de la Auditoría).
- Documentación relacionada a los “Aspectos de Importancia” y/o “Comunicación de Hallazgos” de Auditoría elaborados por los auditores de la Comisión de Auditoría.
- Carta de Representación.
- Papeles de Trabajo correspondiente a la etapa de Ejecución.

5.3 ETAPA DE ELABORACIÓN DEL INFORME DE AUDITORÍA

La etapa de elaboración del Informe de Auditoría representa la tercera etapa de la auditoría gubernamental de sistemas informáticos, tal como, se muestra en el siguiente gráfico:

Etapas de la Auditoría Gubernamental



5.3.1 OBJETIVO

Establecer las diversas actividades que se realizan durante la elaboración del informe de auditoría gubernamental enfocado a los sistemas informáticos.

5.3.2 ACTIVIDADES QUE INCLUYE LA PRESENTE ETAPA:

a. SE INICIA CON:

1. Elaboración del Informe de Auditoría por parte del Auditor Encargado en función de la documentación relacionada a los "Aspectos de Importancia" y/o "Comunicación de Hallazgos" de Auditoría proporcionados por los auditores de la Comisión de Auditoría, los cuales incluyen sus respectivos Papeles de Trabajo. **(NAGU 4.10: ELABORACIÓN DEL INFORME)**

2. El Auditor Encargado elaborará el borrador del informe, sometiendo el mismo a consideración del Supervisor para su revisión.

b. CONTINÚA CON:

3. El Informe de Auditoría deberá adecuarse al cronograma establecido en el "Plan y Programa de Auditoría", con el objetivo de que el Informe de Auditoría sea emitido en el tiempo previsto, de tal forma que su contenido sea oportunamente utilizado por el Titular de la entidad u otras entidades del Estado, tales como, el Congreso de la República y Contraloría General de la República. **(NAGU 4.20: OPORTUNIDAD DEL INFORME)**

4. Para la elaboración del Informe de Auditoría se deberá tener en cuenta lo siguiente:

- Respecto de su redacción: se debe informar los hechos detectados de una manera ordenada, sistemática, constructiva, sencilla y entendible.

- Respecto de su concisión: se debe informar los hechos detectados en forma concreta y exacta.

- Respecto de su exactitud: se debe informar los hechos detectados de tal forma que las evidencias obtenidas en el trabajo de campo de la auditoría sean debidamente confiables y verdaderos, las cuales deben estar debidamente sustentadas a través de los papeles de trabajo.

- Respecto de su objetividad: se debe informar los hechos detectados de manera moderada y prudente que permita una correcta interpretación de las situaciones identificadas producto de la auditoría realizada. **(NAGU 4.30: CARACTERÍSTICAS DEL INFORME)**

5. La Comisión de Auditoría procederá a elaborar el Informe de Auditoría, considerando los puntos que se detallan en el presente cuadro. **(NAGU 4.40: CONTENIDO DEL INFORME)**

	Rubro	**Detalle**
	Denominación	Nombre de la Auditoría
I.	Introducción	
	1. Origen	Razones que motivaron la realización de la auditoría.
	2. Naturaleza y Objetivos	• Tipo de auditoría realizada (Examen Especial). • Objetivos de la auditoría.
	3. Alcance	• Cobertura y profundidad de la auditoría realizada en función de los objetivos trazados en la auditoría. • Incluye el período y áreas de la entidad auditada. • De ser el caso, se consignará las limitaciones de información u otras que hayan afectado la auditoría realizada así como las modificaciones realizadas producto de dichas limitaciones.
	4. Antecedentes y base legal de la entidad	• Aspectos relevantes que estén relacionados con la auditoría. • Principales normas legales aplicadas.
	5. Comunicación de hallazgos	De haberse identificado hallazgos de auditoría, se especificará que se dio cumplimiento a la comunicación de dichos hallazgos realizados al personal comprendido en ellos.
	6. Memorándum de Control Interno	Se especifica si durante la ejecución de la auditoría se emitió el Memorándum de Control Interno. Si fue emitido, éste debe ser anexado al Informe de Auditoría.
	7. Otros aspectos de importancia	Aspectos cuya importancia o significación permiten dan a conocer hechos, acciones o circunstancias que tienen relación con los objetivos de la auditoría.
II.	Observaciones	
	1. Sumilla	Título que identifica el asunto materia de la observación.
	2. Elementos de la observación	• Condición: Hecho ó situación deficiente detectada. • Criterio: Norma, disposición o parámetro de medición aplicable al hecho ó situación observado. • Efecto: Consecuencia real o potencial (cuantitativa o cualitativa) ocasionada por el hecho o situación observado. • Causa: Motivo que dio lugar al hecho o situación observada.
	3. Comentarios y/o aclaraciones del personal comprendido en las observaciones	Respuestas proporcionadas por el personal comprendido en las observaciones, especificando si dicho personal adjuntó documentación

		sustentatoria.
	4. Evaluación de los comentarios y/o aclaraciones presentados	Resultado del análisis realizado por la Comisión de Auditoría respecto de los comentarios y/o aclaraciones del personal comprendido en las observaciones. En concordancia a la Ley N° 29622 y su reglamento[5], se debe incluir la identificación de las presuntas responsabilidades administrativas funcionales por la comisión de infracciones leves, graves y muy graves.
III.	Conclusiones	Argumentos de carácter profesional que se formulan en función de los Aspectos de Importancia y/o Observaciones identificados producto de la auditoría realizada.
IV.	Recomendaciones	Medidas específicas y posibles que se sugieren al Titular y/o Jefaturas de la entidad que permitan superar las causas y deficiencias evidenciadas en la auditoría realizada, las cuales están destinadas a mejorar la gestión de la entidad y contribuir al logro de los objetivos de la entidad en términos de economía, eficiencia y eficacia. En concordancia a la Ley N° 29622 y su reglamento, de haberse identificado presuntas responsabilidades administrativas funcionales por la comisión de infracciones leves, graves y muy graves se debe proceder a: - Recomendar al Titular de la entidad auditada que disponga su procesamiento y la aplicación de sanciones correspondientes en casos de infracciones leves. - Recomendar que el informe sea de conocimiento del Órgano Instructor de la Contraloría General para el inicio del procedimiento sancionador en casos de infracciones graves y muy graves.
V.	Anexos	

[5] *Ley que modifica la Ley N° 27785 y amplía las facultades en el proceso para sancionar en materia de responsabilidad administrativa funcional; publicada el 07.DIC.2010. Así como el Decreto Supremo N° 23-2011-PCM del 18.MAR.2011 que aprueba el Reglamento de la Ley Nº 29622, denominado "Reglamento de infracciones y sanciones para la responsabilidad administrativa funcional derivada de los informes emitidos por los órganos del Sistema Nacional de Control"*

6. Si durante la ejecución de la auditoría de sistemas informáticos se evidencien indicios razonables de comisión de delito (responsabilidad penal) y/o perjuicio económico (responsabilidad civil) se tendrá que efectuar un Informe Especial el cual debe estar técnica y legalmente sustentado. Sobre el particular, cuando se evalúe la responsabilidad civil, sólo de ser el caso (de existir evidencias de dolo[6]) se tendría que evaluar la responsabilidad penal. **(NAGU 4.50: INFORME ESPECIAL)**

Al respecto, se procederá a recomendar en el Informe de Auditoría que a través del área Jurídica de la entidad se dé inicio a las acciones legales correspondientes contra el personal que tuvo participación en los hechos irregulares descritos en el Informe de Auditoría.

En ese sentido, se procede a preparar el Informe Especial, el cual incluye los siguientes puntos:

	Rubro	**Detalle**
	Denominación	Estará identificado como "Informe Especial", el cual debe incluir un título relacionado al tema que se está auditando.
1	Introducción	Se incluye el origen, motivo y alcance de la auditoría (acción de control). Este punto incluye: • Documento de acreditación • Período • Áreas y ámbito geográfico • Normativa que sustente el Informe Especial, entre las cuales, se tiene Ley del Sistema Nacional de Control y Normas de Auditoría Gubernamental.
2	Fundamentos de Hecho	En el caso de responsabilidad penal: Los hechos serán referenciados en términos de indicios. En el caso de responsabilidad civil: el perjuicio económico deberá cuantificarse, especificando que no es posible que la entidad pueda recuperarlo por la vía administrativa.
3	Fundamentos de Derecho	Incluye el análisis del tipo de responsabilidad que se ha identificado correspondiente a los hechos materia de la presunta responsabilidad penal y/o responsabilidad civil incurrida, especificando los artículos del Código Penal y/o Civil u otra normativa aplicable, especificando los plazos de prescripción.
4	Identificación de partícipes en los Hechos	Consiste en individualizar a las personas (que trabajan o trabajaron en la entidad o terceros) involucradas en indicios razonables de comisión de delito.
5	Pruebas	Por cada hecho identificado se deben de adjuntar las pruebas que los sustenten, en forma ordenada y detallada.
6	Recomendación	La recomendación estará en función del tipo

[6] *Voluntad deliberada de cometer un delito a sabiendas de su ilicitud.*

		de responsabilidad determinada (civil y/o penal) con el fin de que se dé inicio a las acciones legales que correspondan.
	Anexos	

7. El Supervisor luego de revisar el Proyecto de Informe conjuntamente con el Auditor Encargado procederán a su sustentación ante el Jefe del Órgano de Control Institucional para su aprobación. Una vez obtenido el visto bueno del Jefe del Órgano de Control Institucional, se procederá al visado, sellado y firmado del Informe Final por parte del Jefe del Órgano de Control Institucional, Supervisor y Auditor Encargado.

c. FINALIZA CON:

8. Remisión del Informe de Auditoría por parte del Jefe del Órgano de Control Institucional al:

- Titular de la Entidad con el fin de que disponga a las unidades organizacionales a su cargo la implementación de las recomendaciones contenidas en el informe. **(NAGU 4.60: SEGUMIENTO DE RECOMENDACIONES DE AUDITORÍAS ANTERIORES)**
- Contraloría General de la República.

5.3.3 ENTREGABLES

- Informe Final de Auditoría
- Informe Especial de Auditoría si es que se identificó responsabilidad civil y/o penal.
- Memorándums de Elevación de remisión del Informe Final de Auditoría al Titular de la entidad y Contraloría General de la República
- Papeles de Trabajo correspondientes a la Etapa de Elaboración del Informe de Auditoría.

ANEXOS DE LA PROPUESTA METODOLÓGICA

ANEXO A-1

CONTROLES DE NORMAS DE CONTROL INTERNO (BASADO EN COSO)

Objetivo: Identificar en forma preliminar los controles y riesgos asociados a los procesos de la entidad que se están auditando, haciendo uso de las normas de control interno.

Referenciado en: Página 73, correspondiente al numeral 9 del literal “b. CONTINUA CON” de la Etapa de Planificación de la Propuesta Metodológica.

Las 32 normas de control interno que conforman los 5 componentes del Sistema Control Interno se detallan a continuación:

1. Ambiente de Control

1.1 Filosofía de la Dirección
1.2 Integridad y valores éticos
1.3 Administración estratégica
1.4 Estructura organizacional
1.5 Administración de los recursos humanos
1.6 Competencia profesional
1.7 Asignación de autoridad y responsabilidad
1.8 Órgano de Control Institucional

2. Evaluación de Riesgos

2.1 Planeamiento de la Administración de riesgos
2.2 Identificación de los riesgos
2.3 Valoración de los riesgos
2.4 Respuesta al riesgo

3. Actividades de Control Gerencial

3.1 Procedimientos de autorización y aprobación
3.2 Segregación de funciones
3.3 Evaluación costo-beneficio
3.4 Controles sobre el acceso a los recursos o archivos
3.5 Verificaciones y Conciliaciones
3.6 Evaluación de desempeño
3.7 Rendición de cuentas
3.8 Documentación de procesos, actividades y tareas
3.9 Revisión de procesos, actividades y tareas
3.10 Controles para las TIC

4. Información y Comunicación

4.1 Funciones y características de la información

ANEXO A-2

RELACIONANDO COBIT 4.1 CON ISO/IEC 27002:2005

Objetivo: Identificar los controles de TI implementados en los procesos de la entidad auditada, haciendo uso de los marcos de referencia COBIT 4.1 e ISO/IEC 27002.

Referenciado en: Página 77, correspondiente al numeral 4 del literal "b. CONTINUA CON" de la Etapa de Ejecución de la Propuesta Metodológica.

Los cuatro (4) dominios de COBIT 4.1 relacionados con los once (11) dominios de ISO/IEC 27002 se detallan a continuación:

DOMINIO: Planificar y Organizar (PO)

COBIT4.1			ISO/IEC 27002:2005
PLANIFICAR Y ORGANIZAR			
PO1	Definir el plan estratégico de TI		-
	PO1.1	Administración del valor de TI	-
	PO1.2	Alineación de TI con el negocio	-
	PO1.3	Evaluación del desempeño y la capacidad actual	-
	PO1.4	Plan estratégico de TI	-
	PO1.5	Planes tácticos de TI	-
	PO1.6	Administración del portafolio de TI	-
PO2	Definir la arquitectura de la información		-
	PO2.1	Modelo de arquitectura de información empresarial	-
	PO2.2	Diccionario de datos empresarial y reglas de sintaxis de datos	7.1.1 Inventario de activos 11.1.1 Políticas de control de acceso
	PO2.3	Esquema de clasificación de datos	7.2.1 Lineamientos para la clasificación 10.7.1 Gestión de medios removibles 10.8.1 Políticas y procedimientos para el intercambio de información 10.8.2 Acuerdos de intercambio 11.1.1 Políticas de control de acceso
	PO2.4	Administración de integridad	-
PO3	Determinar la dirección tecnológica		-
	PO3.1	Planeación de la orientación tecnológica	5.1.2 Revisión de la política de seguridad de la información 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
	PO3.2	Plan de infraestructura tecnológica	-

	PO3.3	Monitoreo de tendencias y regulaciones futuras	6.1.1 Compromiso de la gerencia con la seguridad de la información
	PO3.4	Estándares tecnológicos	10.3.2 Aceptación del sistema 10.8.2 Acuerdos de intercambio 11.7.2 Teletrabajo
	PO3.5	Consejo de arquitectura de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información
PO4	Definir procesos, organización y relaciones de TI		-
	PO4.1	Marco de trabajo de procesos de TI	-
	PO4.2	Comité estratégico de TI	-
	PO4.3	Comité directivo de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.4 Proceso de autorización para las instalaciones de procesamiento de información
	PO4.4	Ubicación organizacional de la función de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad de la información 6.1.4 Proceso de autorización para las instalaciones de procesamiento
	PO4.5	Estructura organizacional de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información
	PO4.6	Establecer roles y responsabilidades	6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.1.1 Roles y responsabilidades 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo 8.2.2 Educación, entrenamiento y concientización en seguridad de información 15.1.4 Protección de datos y privacidad de la información personal
	PO4.7	Responsabilidades para el aseguramiento de la calidad de TI (QA)	-
	PO4.8	Responsabilidad sobre el riesgo, la seguridad y el cumplimiento	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad de la información 8.1.1 Roles y responsabilidades 8.2.1 Responsabilidades de la Gerencia 8.2.3 Procesos disciplinarios 15.1.1 Identificación de legislación aplicable 15.1.2 Derechos de propiedad intelectual 15.1.3 Protección de registros organizacionales 15.1.4 Protección de datos y privacidad de la información personal 15.1.6 Regulación de controles criptográficos 15.2.1 Cumplimiento con políticas y estándares de seguridad
	PO4.9	Propiedad de los datos y sistemas	6.1.3 Asignación de las responsabilidades para la seguridad de la información 6.1.4 Proceso de autorización para las instalaciones de procesamiento de información 7.1.2 Propiedad de los activos 9.2.5 Seguridad de los equipos fuera de las instalaciones

	PO4.10	Supervisión	6.1.2 Coordinación para la seguridad de la información 6.1.3 Asignación de las responsabilidades para la seguridad de la información 7.1.3 Uso aceptable de activos 8.2.1 Responsabilidades de la Gerencia
	PO4.11	Segregación de funciones	8.2.1 Responsabilidades de la Gerencia 10.1.3 Segregación de funciones 10.1.4 Separación de los entornos de desarrollo, pruebas y producción 10.6.1 Controles de red
	PO4.12	Personal de TI	-
	PO4.13	Personal clave de TI	-
	PO4.14	Políticas y procedimientos para el personal contratado	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.3 Considerar la seguridad en los acuerdos con terceros 9.1.5 Trabajo en áreas seguras 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información
	PO4.15	Relaciones	6.1.6 Relación con las autoridades 6.1.7 Relación con grupos de interés especial
PO5	Administrar la inversión en TI		-
	PO5.1	Marco de trabajo para la administración financiera	-
	PO5.2	Priorización dentro del presupuesto de TI	-
	PO5.3	Proceso presupuestal	5.1.2 Revisión de la política de seguridad de la información
	PO5.4	Administración de costos de TI	5.1.2 Revisión de la política de seguridad de la información 13.2.2 Aprendiendo de los incidentes de seguridad de información
	PO5.5	Administración de beneficios	-
PO6	Comunicar las aspiraciones y la dirección de la Gerencia		-
	PO6.1	Política y entorno de control de TI	5.1.1 Documento de la política de seguridad de la información 13.2.1 Responsabilidades y procedimientos

	PO6.2	Riesgo corporativo y marco de referencia del control interno de TI	5.1.1 Documento de la política de seguridad de la información 6.2.2 Considerar la seguridad al tratar con los clientes 7.1.3 Uso aceptable de activos 8.2.2 Educación, entrenamiento y concientización en seguridad de información 8.3.2 Devolución de activos 9.1.5 Trabajo en áreas seguras 9.2.7 Eliminar la propiedad 10.7.3 Procedimientos para el manejo de la información 10.8.1 Políticas y procedimientos para el intercambio de información 10.9.3 Información de dominio público 11.1.1 Políticas de control de acceso 11.3.1 Uso de contraseñas 11.3.2 Equipos desatendidos de Usuario 11.3.3 Políticas de escritorios y pantallas limpias 11.7.1 Computación móvil y las comunicaciones 11.7.2 Teletrabajo 12.3.1 Políticas de uso de controles criptográficos 15.1.2 Derechos de propiedad intelectual 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información 15.2.1 Cumplimiento con políticas y estándares de seguridad
	PO6.3	Administración de políticas para TI	5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.1 Compromiso de la gerencia con la seguridad de la información 8.1.1 Roles y responsabilidades
	PO6.4	Implantación de políticas, estándares y procedimientos de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 6.2.3 Considerar la seguridad en los acuerdos con terceros 8.2.2 Educación, entrenamiento y concientización en seguridad de información
	PO6.5	Comunicación de los objetivos y la dirección de TI	5.1.1 Documento de la política de seguridad de la información 6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información
PO7	Administrar recursos humanos de TI		-
	PO7.1	Reclutamiento y retención del personal	8.1.1 Roles y responsabilidades 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo
	PO7.2	Competencias del personal	8.1.1 Roles y responsabilidades 8.2.2 Educación, entrenamiento y concientización en seguridad de información
	PO7.3	Asignación de roles	8.1.1 Roles y responsabilidades 8.1.3 Términos y condiciones del empleo 8.2.1 Responsabilidades de la Gerencia
	PO7.4	Entrenamiento del personal de TI	8.2.2 Educación, entrenamiento y concientización en seguridad de información
	PO7.5	Dependencia de individuos	-
	PO7.6	Verificación de antecedentes del personal	8.1.2 Verificación

	PO7.7	Evaluación del desempeño del empleado	8.2.2 Educación, entrenamiento y concientización en seguridad de información
	PO7.8	Cambios y ceses en los puestos de trabajo	8.2.3 Procesos disciplinarios 8.3.1 Responsabilidades en el cese 8.3.2 Devolución de activos 8.3.3 Eliminación de privilegios de acceso
PO8	Administrar calidad		-
	PO8.1	Sistema de administración de calidad	-
	PO8.2	Estándares y prácticas de calidad	-
	PO8.3	Estándares para desarrollos y adquisiciones	6.1.5 Acuerdos de confidencialidad 6.2.3 Considerar la seguridad en los acuerdos con terceros 12.5.5 Outsourcing de desarrollo de software
	PO8.4	Enfoque en el cliente de TI	-
	PO8.5	Mejora continua	-
	PO8.6	Medición, monitoreo y revisión de la calidad	-
PO9	Evaluar y administrar riesgos de TI		-
	PO9.1	Marco de trabajo de administración de riesgos	14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos
	PO9.2	Establecimiento del contexto del riesgo	14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos
	PO9.3	Identificación de eventos	13.1.1 Reporte de eventos de seguridad de información 13.1.2 Reporte de debilidades de seguridad
	PO9.4	Evaluación de riesgos de TI	5.1.2 Revisión de la política de seguridad de la información 14.1.2 Continuidad del negocio y evaluación de riesgos
	PO9.5	Respuesta a los riesgos	-
	PO9.6	Mantenimiento y monitoreo de un plan de acción de riesgos	-
P10	Administrar proyectos		-
	PO10.1	Marco de trabajo para la administración de programas	-
	PO10.2	Marco de trabajo para la administración de proyectos	-
	PO10.3	Enfoque de administración de proyectos	-
	PO10.4	Compromiso de los interesados	-
	PO10.5	Declaración de alcance del proyecto	-
	PO10.6	Inicio de las fases del proyecto	-
	PO10.7	Plan integrado del proyecto	-
	PO10.8	Recursos del proyecto	-
	PO10.9	Administración de riesgos del proyecto	-
	PO10.10	Plan de calidad del proyecto	-
	PO10.11	Control de cambios del proyecto	-
	PO10.12	Planeamiento del proyecto y métodos de aseguramiento	-

	PO10.13	Medición del desempeño, reporte y monitoreo del proyecto	-
	PO10.14	Cierre del proyecto	-

Fuente Cobit 4.1

DOMINIO: Adquirir e Implantar (AI)

COBIT 4.1			ISO/IEC 27002:2005
ADQUIRIR E IMPLANTAR			
AI1	Identificar soluciones automatizadas.		-
	AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.	8.2.2 Educación, entrenamiento y concientización en seguridad de información 12.1.1 Análisis y especificación de los requisitos de seguridad 10.3.2 Aceptación del sistema
	AI1.2	Reporte de análisis de riesgos	11.6.2 Aislamiento de sistemas sensitivos 12.1.1 Análisis y especificación de los requisitos de seguridad
	AI1.3	Estudio de factibilidad y formulación de cursos alternativos de acción	-
	AI1.4	Requerimientos, decisión de factibilidad y aprobación.	6.1.4 Proceso de autorización para las instalaciones de procesamiento de información 10.3.2 Aceptación del sistema
AI2	Adquirir y mantener el software aplicativo.		-
	AI2.1	Diseño de alto nivel	-
	AI2.2	Diseño detallado	-
	AI2.3	Control y auditabilidad de las aplicaciones	10.10.1 Logs de auditoría 10.10.5 Logs de fallas 12.2.1 Validación de datos de entrada 12.2.2 Control de procesamiento interno 12.2.3 Integridad de mensajes 12.2.4 Validación de datos de salida 13.2.3 Recolección de evidencia 15.3.1 Controles de auditoría de sistemas de información 15.3.2 Protección de herramientas de auditoría de sistemas de información
	AI2.4	Seguridad y disponibilidad de las aplicaciones.	6.1.4 Proceso de autorización para las instalaciones de procesamiento de información 7.2.1 Lineamientos para la clasificación 10.3.2 Aceptación del sistema 11.6.2 Aislamiento de sistemas sensitivos 12.1.1 Análisis y especificación de los requisitos de seguridad 12.2.3 Integridad de mensajes 12.3.1 Política de uso de controles criptográficos 12.4.3 Control de acceso al código fuente de los programas 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 12.5.4 Fuga de información 15.3.2 Protección de herramientas de auditoría de sistemas de información
	AI2.5	Configuración e implementación de software aplicativo adquirido	12.5.3 Restricciones en los cambios a los paquetes de software
	AI2.6	Actualizaciones importantes en sistemas existentes	12.5.1 Procedimientos de control de cambios
	AI2.7	Desarrollo de software aplicativo	12.5.5 Outsourcing de desarrollo de software
	AI2.8	Aseguramiento de la calidad del software	10.3.2 Aceptación del sistema
	AI2.9	Administración de los requisitos de las aplicaciones	-

	AI2.10	Mantenimiento del software aplicativo	-
AI3	Adquirir y mantener la infraestructura tecnológica		-
	AI3.1	Plan de adquisición de infraestructura tecnológica	-
	AI3.2	Protección y disponibilidad de la infraestructura	12.1.1 Análisis y especificación de los requisitos de seguridad
	AI3.3	Mantenimiento de la Infraestructura	9.1.5 Trabajo en áreas seguras 9.2.4 Mantenimiento de equipos 12.4.2 Protección de los datos de prueba de sistema 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 12.6.1 Control de vulnerabilidades técnicas
	AI3.4	Ambiente de prueba de factibilidad	10.1.4 Separación de los entornos de desarrollo, pruebas y producción
AI4	Facilitar la operación y el uso.		-
	AI4.1	Planificación de soluciones operacionales	-
	AI4.2	Transferencia de conocimiento a la Gerencia del negocio	-
	AI4.3	Transferencia de conocimiento a los usuarios finales	-
	AI4.4	Transferencia de conocimiento al personal de operaciones y soporte	10.1.1 Procedimientos operativos documentados 10.3.2 Aceptación del sistema 10.7.4 Seguridad de la documentación de sistemas 13.2.2 Aprendiendo de los incidentes de seguridad de información
AI5	Adquirir recursos de TI.		-
	AI5.1	Control de adquisiciones	6.1.5 Acuerdos de confidencialidad
	AI5.2	Administración de contratos de proveedores	6.1.5 Acuerdos de confidencialidad 6.2.3 Considerar la seguridad en los acuerdos con terceros 10.8.2 Acuerdos de intercambio 12.5.5 Outsourcing de desarrollo de software
	AI5.3	Selección de proveedores	-
	AI5.4	Adquisición de recursos de TI	-
AI6	Administrar cambios.		-
	AI6.1	Estándares y procedimientos para cambios	10.1.2 Gestión de cambios 12.5.3 Restricciones en los cambios a los paquetes de software
	AI6.2	Evaluación de impacto, priorización y autorización	10.1.2 Gestión de cambios 12.5.1 Procedimientos de control de cambios 12.5.3 Restricciones en los cambios a los paquetes de software 12.6.1 Control de vulnerabilidades técnicas
	AI6.3	Cambios de emergencia	10.1.2 Gestión de cambios 11.5.4 Uso de utilitarios del sistema 12.5.1 Procedimiento de control de cambios 12.5.3 Restricciones en los cambios a los paquetes de software 12.6.1 Control de vulnerabilidades técnicas
	AI6.4	Seguimiento y reporte de estado de los cambios	10.1.2 Gestión de cambios
	AI6.5	Cierre y documentación del cambio	10.1.2 Gestión de cambios
AI7	Instalar y acreditar soluciones y cambios.		-
	AI7.1	Entrenamiento	8.2.2 Educación, entrenamiento y concientización en seguridad de información
	AI7.2	Plan de pruebas	12.5.1 Procedimientos de control de cambios 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo

	AI7.3	Plan de implementación	-
	AI7.4	Ambiente de prueba	10.1.4 Separación de los entornos de desarrollo, pruebas y producción 12.4.3 Control de acceso al código fuente de los programas 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo
	AI7.5	Conversión de datos y sistemas	-
	AI7.6	Pruebas de cambios	6.1.4 Proceso de autorización para las instalaciones de procesamiento de información 12.4.3 Control de acceso al código fuente de los programas 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo
	AI7.7	Pruebas de aceptación final	10.3.2 Aceptación del sistema 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 12.5.4 Fuga de información
	AI7.8	Promoción a producción	-
	AI7.9	Revisión posterior a la implementación	-

Fuente Cobit 4.1

DOMINIO: Entregar y Dar Soporte (DS)

COBIT4.1			ISO/IEC 27002:2005
ENTREGAR Y DAR SOPORTE			
DS1	Definir y administrar niveles de servicio.		-
	DS1.1	Marco de administración de niveles de servicio	10.2.1 Entrega de servicios
	DS1.2	Definiciones de los servicios	10.2.1 Entrega de servicios
	DS1.3	Acuerdos de niveles de servicio (ANS)	10.2.1 Entrega de servicios
	DS1.4	Acuerdos de niveles de operación	-
	DS1.5	Monitoreo y reporte del cumplimento de los niveles de servicio	10.2.2 Monitoreo y revisión de los servicios de terceros 10.2.3 Gestión de cambios a los servicios de terceros
	DS1.6	Revisión de los acuerdos de niveles de servicio y de los contratos	-
DS2	Administrar servicios de terceros.		-
	DS2.1	Identificación de todas las relaciones con proveedores	6.2.1 Identificación de riesgos relacionados con terceros
	DS2.2	Administración de relaciones con proveedores	6.2.3 Considerar la seguridad en los acuerdos con terceros 10.2.3 Gestión de cambios a los servicios de terceros 15.1.4 Protección de datos y privacidad de la información personal
	DS2.3	Administración de riesgos de proveedores	6.2.1 Identificación de riesgos relacionados con terceros 6.2.3 Considerar la seguridad en los acuerdos con terceros 8.1.2 Verificación 8.1.3 Términos y condiciones del empleo 10.2.3 Gestión de cambios a los servicios de terceros 10.8.2 Acuerdos de intercambio
	DS2.4	Monitoreo del desempeño de proveedores	6.2.3 Considerar la seguridad en los acuerdos con terceros 10.2.1 Entrega de servicios 10.2.2 Monitoreo y revisión de los servicios de terceros 12.4.2 Protección de los datos de prueba del sistema 12.5.5 Outsourcing de desarrollo de software
DS3	Administrar desempeño y capacidad.		-
	DS3.1	Planeamiento del desempeño y la capacidad	10.3.1 Gestión de la capacidad
	DS3.2	Capacidad y desempeño actual	10.3.1 Gestión de la capacidad
	DS3.3	Capacidad y desempeño futuro	10.3.1 Gestión de la capacidad
	DS3.4	Disponibilidad de recursos de TI	-
	DS3.5	Monitoreo y reporte	-
DS4	Garantizar la continuidad del servicio.		-
	DS4.1	Marco de trabajo de continuidad de TI	6.1.6 Relación con las autoridades 6.1.7 Relación con grupos de interés especial 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos 14.1.4 Marco de planificación de continuidad del negocio
	DS4.2	Planes de continuidad de TI	6.1.6 Relación con las autoridades 6.1.7 Relación con grupos de interés especial 14.1.3 Desarrollar e implementar planes de continuidad que incluyan la seguridad de la información
	DS4.3	Recursos críticos de TI	14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.2 Continuidad del negocio y evaluación de riesgos

	DS4.4	Mantenimiento del plan de continuidad de TI	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
	DS4.5	Pruebas del plan de continuidad de TI	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
	DS4.6	Entrenamiento en el plan de continuidad de TI	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
	DS4.7	Distribución del plan de continuidad de TI	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
	DS4.8	Recuperación y reanudación de los servicios de TI	14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.3 Mantener o restaurar operaciones para asegurar la disponibilidad de la información
	DS4.9	Almacenamiento externo y respaldos	10.5.1 Respaldo de la información
	DS4.10	Revisión post-reanudación	14.1.5 Pruebas, mantenimiento y revaluación de los planes de continuidad del negocio
DS5	Garantizar la seguridad de los sistemas.		-
	DS5.1	Administración de la seguridad de TI	6.1.1 Compromiso de la gerencia con la seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.2.3 Considerar la seguridad en los acuerdos con terceros 8.2.2 Educación, entrenamiento y concientización en seguridad de información
	DS5.2	Plan de seguridad de TI	5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.2.2 Educación, entrenamiento y concientización en seguridad de información 11.1.1 Políticas de control de acceso 11.7.1 Computación móvil y las comunicaciones 11.7.2 Teletrabajo
	DS5.3	Administración de identidad	5.1.1 Documento de la política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.2 Coordinación para la seguridad de la información 6.1.5 Acuerdos de confidencialidad 8.2.2 Educación, entrenamiento y concientización en seguridad de información 11.1.1 Políticas de control de acceso 11.7.1 Computación móvil y las comunicaciones 11.7.2 Teletrabajo
	DS5.4	Administración de cuentas del usuario	6.1.5 Acuerdos de confidencialidad 6.2.1 Identificación de riesgos relacionados con terceros 6.2.2 Considerar la seguridad a tratar con los clientes 8.1.1 Roles y responsabilidades 8.3.1 Responsabilidades en el cese 8.3.3 Eliminación de privilegios de acceso 10.1.3 Segregación de funciones 11.1.1 Políticas de control de acceso 11.2.1 Registro de usuarios 11.2.2 Gestión de privilegios 11.2.4 Revisión de derechos de acceso de usuarios 11.3.1 Uso de contraseñas 11.5.1 Procedimientos seguros de inicio de sesión 11.5.3 Sistema de gestión de contraseñas 11.6.1 Restricción de acceso a la información
	DS5.5	Pruebas, vigilancia y monitoreo de la seguridad	6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema 10.10.3 Protección de logs 10.10.4 Logs de administrador y de operador 12.6.1 Control de vulnerabilidades técnicas 13.1.2 Reporte de debilidades de seguridad 15.2.2 Verificación de cumplimiento técnico 15.3.1 Controles de auditoría de sistemas de información

	DS5.6	Definición de incidente de seguridad	8.2.3 Procesos disciplinarios 13.1.1 Reporte de eventos de seguridad de información 13.1.2 Reporte de debilidades de seguridad 13.2.1 Responsabilidades y procedimientos 13.2.3 Recolección de evidencia
	DS5.7	Protección de la tecnología de seguridad	6.1.4 Proceso de autorización para las instalaciones de procesamiento de información 9.1.6 Áreas de acceso público, despacho y recepción 9.2.1 Ubicación y protección de equipos 9.2.3 Seguridad del cableado 10.6.2 Seguridad de los servicios de red 10.7.4 Seguridad de la documentación de sistemas 10.10.1 Logs de auditoría 10.10.3 Protección de logs 10.10.4 Logs de administrador y de operador 10.10.5 Logs de fallas 10.10.6 Sincronización de relojes 11.3.2 Equipos desatendidos de usuario 11.3.3 Políticas de escritorios y pantallas limpias 11.4.3 Identificación de equipos en redes 11.4.4 Protección de puertos de configuración y diagnóstico remoto 11.5.1 Procedimientos seguros de inicio de sesión 11.5.4 Uso de utilitarios del sistema 11.5.5 Período de inactividad de sesión 11.5.6 Limitación del tiempo de conexión 11.6.2 Aislamiento de sistemas sensitivos 11.7.1 Computación móvil y las comunicaciones 11.7.2 Teletrabajo 12.4.1 Control del software de operaciones 12.6.1 Control de vulnerabilidades técnicas 13.1.2 Reporte de debilidades de seguridad 13.2.3 Recolección de evidencia 15.2.2 Verificación de cumplimiento técnico 15.3.2 Protección de las herramientas de auditoría de sistemas
	DS5.8	Administración de llaves criptográficas	10.8.4 Mensajería electrónica 12.2.3 Integridad de mensajes 12.3.1 Política de uso de controles criptográficos 12.3.2 Gestión de llaves 15.1.6 Regulación de controles criptográficos
	DS5.9	Prevención, detección y corrección de software malicioso	10.4.1 Controles contra código malicioso 10.4.2 Controles contra código móvil
	DS5.10	Seguridad de la red	6.2.1 Identificación de riesgos relacionados con terceros 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.4.1 Política de uso de los servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 11.4.3 Identificación de equipos en redes 11.4.4 Protección de puertos de configuración y diagnóstico remoto 11.4.5 Segregación en redes 11.4.6 Control de conexiones en la red 11.4.7 Control de enrutamiento en la red 11.6.2 Aislamiento de sistemas sensitivos
	DS5.11	Intercambio de datos sensitivos	6.2.1 Identificación de riesgos relacionados con terceros 10.6.1 Controles de red 10.6.2 Seguridad de los servicios de red 11.4.1 Política de uso de los servicios de red 11.4.2 Autenticación de usuarios para conexiones externas 11.4.3 Identificación de equipos en redes 11.4.4 Protección de puertos de configuración y diagnóstico remoto 11.4.5 Segregación en redes 11.4.6 Control de conexiones en la red 11.4.7 Control de enrutamiento en la red 11.6.2 Aislamiento de sistemas sensitivos
DS6	Identificar y asignar costos.		-
	DS6.1	Definición de servicios	-
	DS6.2	Contabilización de TI	-
	DS6.3	Modelamiento de costos y cargos	-

	DS6.4	Mantenimiento del modelo de costos	-
DS7	Educar y entrenar a los usuarios.		-
	DS7.1	Identificación de necesidades de educación y formación	8.2.2 Educación, entrenamiento y concientización en seguridad de información
	DS7.2	Brindar educación y entrenamiento	8.2.2 Educación, entrenamiento y concientización en seguridad de información
	DS7.3	Evaluación del entrenamiento recibido	-
DS8	Administrar la mesa de servicio y los incidentes.		-
	DS8.1	Mesa de Servicios	14.1.4 Marco de planeamiento de continuidad del negocio
	DS8.2	Registro de consultas de clientes	13.1.1 Reporte de eventos de seguridad de información 13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos 13.2.1 Responsabilidades y procedimientos 13.2.3 Recolección de evidencia
	DS8.3	Escalamiento de incidentes	13.1.2 Se pueden agregar los reportes de debilidades de seguridad ya que se relacionan con la identificación de eventos 13.2.3 Recolección de evidencia 14.1.1 Incluir la seguridad de información en el proceso de gestión de continuidad del negocio 14.1.4 Marco de planificación de continuidad del negocio
	DS8.4	Cierre de incidentes	13.2.2 Aprendiendo de los incidentes de seguridad de información 13.2.3 Recolección de evidencia
	DS8.5	Reportes y análisis de tendencias	13.2.2 Aprendiendo de los incidentes de seguridad de información
DS9	Administrar la configuración.		-
	DS9.1	Repositorio y línea base de configuración	7.2.2 Etiquetado y manejo de la información 12.4.1 Control del software de operaciones 12.4.2 Protección de los datos de prueba de sistema
	DS9.2	Identificación y mantenimiento de elementos de configuración	7.1.1 Inventario de activos 7.1.2 Propiedad de los activos 7.2.2 Etiquetado y manejo de la información 10.7.4 Seguridad de la documentación de sistemas 11.4.3 Identificación de equipos en redes 12.4.2 Protección de los datos de prueba de sistema 12.5.3 Restricciones en los cambios a los paquetes de software 12.6.1 Control de vulnerabilidades técnicas 15.1.5 Prevención del uso indebido de instalaciones de
	DS9.3	Revisión de integridad de la configuración	7.1.1 Inventario de activos 10.7.4 Seguridad de la documentación de sistemas 12.5.2 Revisión técnica de las aplicaciones luego de cambios en el sistema operativo 15.1.5 Prevención del uso indebido de instalaciones de procesamiento de información
DS10	Administrar los problemas.		-
	DS10.1	Identificación y clasificación de problemas	13.2.2 Aprendiendo de los incidentes de seguridad de información
	DS10.2	Seguimiento y resolución de problemas	13.2.2 Aprendiendo de los incidentes de seguridad de información
	DS10.3	Cierre de problemas	-
	DS10.4	Integración de la administración de configuración, incidentes y problemas	-
DS11	Administrar los datos.		-
	DS11.1	Requerimientos del negocio para la administración de datos	10.8.1 Políticas y procedimientos para el intercambio de información
	DS11.2	Acuerdos para el almacenamiento y la conservación	10.5.1 Respaldo de la información 10.7.1 Gestión de medios removibles 15.1.3 Protección de registros organizacionales
	DS11.3	Sistema de administración de librerías de medios	10.7.1 Gestión de medios removibles 10.7.2 Eliminación de medios 12.4.3 Control de acceso al código fuente de los programas
	DS11.4	Eliminación	9.2.6 Eliminación o reutilización segura de equipos 10.7.1 Gestión de medios removibles 10.7.2 Eliminación de medios

	DS11.5	Respaldo y restauración	10.5.1 Respaldo de la información
	DS11.6	Requisitos de seguridad para la administración de datos	10.5.1 Respaldo de la información 10.7.3 Procedimientos para el manejo de la información 10.8.3 Medios de almacenamiento físico en tránsito 10.8.4 Mensajería electrónica 12.4.2 Protección de datos de prueba de sistema 12.4.3 Control de acceso al código fuente de los programas
DS12	Administrar el ambiente físico.		-
	DS12.1	Selección y diseño del centro de datos	9.1.1 Perímetro de seguridad física 9.1.3 Seguridad de oficinas, salas e instalaciones 9.1.6 Áreas de acceso público, despacho y recepción
	DS12.2	Medidas de seguridad física	9.1.1 Perímetro de seguridad física 9.1.2 Controles físicos de ingreso 9.1.3 Seguridad de oficinas, salas e instalaciones 9.2.5 Seguridad de los equipos fuera de las instalaciones 9.2.7 Eliminar la propiedad
	DS12.3	Acceso Físico	6.2.1 Identificación de riesgos relacionados con terceros 9.1.2 Controles físicos de ingreso 9.1.5 Trabajo en áreas seguras 9.1.6 Áreas de acceso público, despacho y recepción 9.2.5 Seguridad de los equipos fuera de las instalaciones
	DS12.4	Protección contra factores ambientales	9.1.4 Protección contra amenazas externas y ambientales 9.2.1 Ubicación y protección de equipos 9.2.2 Servicios de soporte 9.2.3 Seguridad del cableado
	DS12.5	Administración de instalaciones físicas	9.2.2 Servicios de soporte 9.2.4 Mantenimiento de equipos
DS13	Administrar las operaciones.		-
	DS13.1	Procedimientos e instrucciones de operación	10.1.1 Procedimientos operativos documentados 10.7.4 Seguridad de la documentación de sistemas
	DS13.2	Programación de tareas	-
	DS13.3	Monitoreo de la infraestructura de TI	-
	DS13.4	Documentos sensitivos y dispositivos de salida	-
	DS13.5	Mantenimiento preventivo del hardware	9.2.4 Mantenimiento de equipos

Fuente Cobit 4.1

DOMINIO: Monitorear y Evaluar (ME)

COBIT 4.1			ISO/IEC 27002:2005
MONITOREAR Y EVALUAR			
ME1	Monitorear y evaluar el desempeño de TI.		-
	ME1.1	Enfoque del Monitoreo	-
	ME1.2	Definición y recolección de datos de monitoreo	10.10.2 Monitoreo del uso del sistema
	ME1.3	Método de monitoreo	-
	ME1.4	Evaluación del desempeño	-
	ME1.5	Reportes al Consejo Directivos y a ejecutivos	-
	ME1.6	Acciones correctivas	-
ME2	Monitorear y evaluar el control interno		-
	ME2.1	Monitoreo del marco de trabajo del control interno	5.1.1 Documento de la política de seguridad de la información 15.2.1 Cumplimiento con políticas y estándares de seguridad.
	ME2.2	Revisiones de Supervisión	5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema 10.10.4 Logs de administrador y de operador 15.2.1 Cumplimiento con políticas y estándares de seguridad
	ME2.3	Excepciones de control	15.2.1 Cumplimiento con políticas y estándares de seguridad
	ME2.4	Autoevaluación de control	15.2.1 Cumplimiento con políticas y estándares de seguridad
	ME2.5	Aseguramiento del control interno	5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema 10.10.4 Logs de administrador y de operador 15.2.1 Cumplimiento con políticas y estándares de seguridad 15.2.2 Verificación de cumplimiento técnico 15.3.1 Controles de auditoría de sistemas de información
	ME2.6	Control interno para terceros	6.2.3 Considerar la seguridad en los acuerdos con terceros 10.2.2 Monitoreo y revisión de los servicios de terceros 15.2.1 Cumplimiento con políticas y estándares de seguridad
	ME2.7	Acciones correctivas	5.1.2 Revisión de la política de seguridad de la información 15.2.1 Cumplimiento con políticas y estándares de seguridad
ME3	Garantizar cumplimiento regulatorio.		-
	ME3.1	Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales	6.1.6 Relación con las autoridades que tengan impacto potencial en TI 15.1.1 Identificación de legislación aplicable 15.1.2 Derechos de propiedad intelectual 15.1.4 Protección de datos y privacidad de la información personal
	ME3.2	Optimizar la Respuesta a Requerimientos Externos	-

	ME3.3	Evaluación del Cumplimiento con Requerimientos Externos	6.1.6 Relación con las autoridades que tengan impacto potencial en TI 15.1.1 Identificación de legislación aplicable 15.1.2 Derechos de propiedad intelectual 15.1.4 Protección de datos y privacidad de la información personal
	ME3.4	Aseguramiento Positivo del Cumplimiento	6.1.6 Relación con las autoridades que tengan impacto potencial en TI 15.1.1 Identificación de legislación aplicable 15.1.2 Derechos de propiedad intelectual 15.1.4 Protección de datos y privacidad de la información personal
	ME3.5	Reportes Integrados	-
ME4	Proporcionar gobierno de TI.		-
	ME4.1	Establecer un marco de trabajo de gobierno para TI	-
	ME4.2	Alineamiento estratégico	-
	ME4.3	Entrega de valor	-
	ME4.4	Administración de recursos	-
	ME4.5	Administración de riesgos	-
	ME4.6	Medición del desempeño	-
	ME4.7	Aseguramiento independiente	5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 10.10.2 Monitoreo del uso del sistema

Fuente Cobit 4.1

ANEXO A-3

RELACIONANDO ISO/IEC 27002:2005 CON COBIT 4.1

Objetivo: Identificar los controles de TI implementados en los procesos de la entidad auditada, haciendo uso de los marcos de referencia ISO/IEC 27002 y COBIT 4.1.

Referenciado en: Página 77, correspondiente al numeral 4 del literal "b. CONTINUA CON" de la Etapa de Ejecución de la Propuesta Metodológica.

Los once (11) dominios de ISO/IEC 27002 relacionados con los cuatro (4) dominios de COBIT 4.1, se detallan a continuación:

ISO/IEC 27002:2005			COBIT4.1
5.0 POLÍTICA DE SEGURIDAD			
5.1	Políticas de seguridad de la información		-
	5.1.1	Documento de la política de seguridad de información	PO6.1 Política y entorno de control de TI PO6.2 Riesgo corporativo y marco de referencia del control interno de TI PO6.3 Gestión de políticas de TI PO6.5 Comunicación de los objetivos y la dirección de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad ME2.1 Monitoreo del marco de trabajo
	5.1.2	Revisión de la política de seguridad de la información	PO3.1 Planeamiento de la orientación tecnológica PO5.3 Proceso presupuestal PO5.4 Gestión de costos de TI PO6.3 Gestión de políticas de TI PO9.4 Evaluación de riesgos de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad ME2.2 Revisiones de supervisión ME2.5 Aseguramiento del control interno ME2.7 Acciones correctivas ME4.7 Aseguramiento independiente
6.0 ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN			**-**
6.1	Organización interna		-
	6.1.1	Compromiso de la gerencia con la seguridad de la información	PO3.3 Monitoreo de tendencias y regulaciones futuras PO3.5 Consejo de arquitectura de TI PO4.3 Comité directivo de TI PO4.4 Ubicación organizacional de la función de TI PO4.5 Estructura organizacional de TI PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento PO6.3 Gestión de políticas de TI PO6.4 Implantación de políticas, estándares y procedimientos PO6.5 Comunicación de los objetivos y la dirección de TI DS5.1 Gestión de la seguridad de TI

	6.1.2	Coordinación para la seguridad de la información	PO4.4 Ubicación organizacional de la función de TI PO4.5 Estructura organizacional de TI PO4.6 Establecer roles y responsabilidades PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento PO4.10 Supervisión PO6.5 Comunicación de los objetivos y la dirección de TI DS5.1 Gestión de la seguridad de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad
	6.1.3	Asignación de las responsabilidades para la seguridad de la información	PO4.4 Ubicación organizacional de la función de TI PO4.6 Establecer roles y responsabilidades PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento PO4.9 Propiedad de los datos y sistemas PO4.10 Supervisión
	6.1.4	Proceso de autorización para las instalaciones de procesamiento de información	PO4.3 Comité directivo de TI PO4.4 Ubicación organizacional de la función de TI PO4.9 Propiedad de los datos y sistemas AI1.4 Requerimientos, decisión de factibilidad y aprobación AI2.4 Seguridad y disponibilidad de las aplicaciones AI7.6 Pruebas de cambios DS5.7 Protección de la tecnología de seguridad
	6.1.5	Acuerdos de confidencialidad	PO4.6 Establecer roles y responsabilidades PO4.14 Políticas y procedimientos para el personal contratado PO8.3 Estándares para desarrollos y adquisiciones AI5.1 Control de adquisiciones AI5.2 Gestión de contratos con proveedores DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad DS5.4 Gestión de cuentas de usuario
	6.1.6	Relación con las autoridades	PO4.15 Relaciones DS4.1 Marco de trabajo de continuidad de TI DS4.2 Planes de continuidad de TI ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual ME3.3 Evaluación del cumplimiento con requerimientos externos ME3.4 Aseguramiento positivo del cumplimiento
	6.1.7	Relación con grupos de interés especial	PO4.15 Relaciones DS4.1 Marco de trabajo de continuidad de TI DS4.2 Planes de continuidad de TI
	6.1.8	Revisión independiente de la seguridad de la información	PO6.4 Implantación de políticas, estándares y procedimientos DS5.5 Pruebas, vigilancia y monitoreo de la seguridad ME2.2 Revisiones de supervisión ME2.5 Aseguramiento del control interno ME4.7 Aseguramiento independiente
6.2	Entidades externas		-
	6.2.1	Identificación de riesgos relacionados con terceros	PO4.14 Políticas y procedimientos para personal contratado DS2.1 Identificación de todas las relaciones con proveedores DS2.3 Gestión de riesgos de proveedores DS5.4 Gestión de cuentas de usuario DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos DS12.3 Acceso físico
	6.2.2	Considerar la seguridad al tratar con los clientes	PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI DS5.4 Gestión de cuentas de usuarios
	6.2.3	Considerar la seguridad en acuerdos con terceros	PO4.14 Políticas y procedimientos para personal contratado PO6.4 Implantación de políticas, estándares y procedimientos PO8.3 Estándares para desarrollos y adquisiciones AI5.2 Gestión de contratos con proveedores DS2.2 Gestión de relaciones con proveedores DS2.3 Gestión de riesgos de proveedores DS2.4 Monitoreo del desempeño de proveedores DS5.1 Gestión de la seguridad de TI ME2.6 Control interno para terceros

7.0 GESTIÓN DE LOS ACTIVOS			**-**
7.1	Responsabilidad sobre los activos		-
	7.1.1	Inventario de activos	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de los datos DS9.2 Identificación y mantenimiento de elementos de la configuración DS9.3 Revisión de integridad de la configuración
	7.1.2	Propiedad de los Activos	PO4.9 Propiedad de los datos y sistemas DS9.2 Identificación y mantenimiento de elementos de la configuración
	7.1.3	Uso aceptable de Activos	PO4.10 Supervisión PO6.2 Riesgo corporativo y marco de referencia del control interno de TI
7.2	Clasificación de la información		
	7.2.1	7.2.1 Lineamientos para la clasificación	PO2.3 Esquema de clasificación de datos AI2.4 Seguridad y disponibilidad de las aplicaciones
	7.2.2	7.2.2 Etiquetado y manejo de la información	DS9.1 Repositorio y línea base de configuración
8.0 SEGURIDAD DEL PERSONAL			**-**
8.1	Antes de la contratación de personal		-
	8.1.1	Roles y responsabilidades	PO4.6 Establecer roles y responsabilidades PO4.8 Responsabilidad sobre riesgo, la seguridad y el cumplimiento PO6.3 Gestión de políticas de TI PO7.1 Reclutamiento y retención del personal PO7.2 Competencias del personal PO7.3 Asignación de roles DS5.4 Gestión de cuentas de usuario
	8.1.2	Verificación	PO4.6 Establecer roles y responsabilidades PO7.1 Reclutamiento y retención del personal PO7.6 Verificación de antecedentes del personal DS2.3 Gestión de riesgos de proveedores
	8.1.3	Términos y condiciones del empleo	PO4.6 Establecer roles y responsabilidades PO7.1 Reclutamiento y retención del personal PO7.3 Asignación de roles DS2.3 Gestión de riesgos de proveedores
8.2	Durante el Empleo		**-**
	8.2.1	Responsabilidades de la Gerencia	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento PO4.10 Supervisión PO4.11 Segregación de funciones PO7.3 Asignación de roles
	8.2.2	Educación, entrenamiento y concientización en seguridad de información	PO4.6 Establecer roles y responsabilidades PO6.2 Riesgo corporativo y marco de referencia del control interno de TI PO6.4 Implantación de políticas, estándares y procedimientos PO7.2 Competencias del personal PO7.4 Entrenamiento del personal de TI PO7.7 Evaluación del desempeño del empleado AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio AI7.1 Entrenamiento DS5.1 Gestión de la seguridad de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad DS7.1 Identificación de las necesidades de educación y entrenamiento DS7.2 Brindar educación y entrenamiento
	8.2.3	Procesos disciplinarios	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento PO7.8 Cambios y ceses en los puestos de trabajo DS5.6 Definición de incidente de seguridad
8.3	Cambios y ceses en el empleo		**-**
	8.3.1	Responsabilidades en el cese	PO7.8 Cambios y ceses en los puestos de trabajo DS5.4 Gestión de cuentas de usuario
	8.3.2	Devolución de activos	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI PO7.8 Cambios y ceses en los puestos de trabajo

	8.3.3	Eliminación de privilegios de acceso	PO7.8 Cambios y ceses en los puestos de trabajo DS5.4 Gestión de cuentas de usuario
9.0 SEGURIDAD FÍSICA Y AMBIENTAL			**-**
9.1	Asegurar las áreas		-
	9.1.1	Perímetro de seguridad física	DS12.1 Selección y diseño del centro de datos DS12.2 Medidas de seguridad física
	9.1.2	Controles físicos de ingreso	DS12.2 Medidas de seguridad física DS12.3 Acceso físico
	9.1.3	Seguridad de oficinas, salas e instalaciones	DS12.1 Selección y diseño del centro de datos DS12.2 Medidas de seguridad física
	9.1.4	Protección contra amenazas externas y ambientales	DS12.4 Protección contra factores ambientales
	9.1.5	Trabajo en áreas seguras	PO4.14 Políticas y procedimientos para personal contratado PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI AI3.3 Mantenimiento de la infraestructura DS12.3 Acceso físico
	9.1.6	Áreas de acceso público, despacho y recepción	DS5.7 Protección de la tecnología de seguridad DS12.1 Selección y diseño del centro de datos DS12.3 Acceso físico
9.2	Seguridad de los equipos		-
	9.2.1	Ubicación y protección de los equipos	DS5.7 Protección de la tecnología de seguridad DS12.4 Protección contra factores ambientales
	9.2.2	Servicios de soporte	DS12.4 Protección contra factores ambientales DS12.5 Gestión de instalaciones físicas
	9.2.3	Seguridad del cableado	DS5.7 Protección de la tecnología de seguridad DS12.4 Protección contra factores ambientales
	9.2.4	Mantenimiento de equipos	AI3.3 Mantenimiento de la infraestructura DS12.5 Gestión de instalaciones físicas DS13.5 Mantenimiento preventivo del hardware
	9.2.5	Seguridad de los equipos fuera de las instalaciones	PO4.9 Propiedad de los datos y sistemas DS12.2 Medidas de seguridad física DS12.3 Acceso físico
	9.2.6	Eliminación o reutilización segura de equipos	DS11.4 Desechar
	9.2.7	Eliminar la propiedad	PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI DS12.2 Medidas de seguridad física
10.0 GESTIÓN DE COMUNICACIONES Y LAS OPERACIONES			**-**
10.1	Responsabilidades y procedimientos operacionales		-
	10.1.1	Procedimientos operativos documentados	AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio AI4.4 Transferencia del conocimiento al personal de operaciones y soporte DS13.1 Procedimientos e instrucciones de operación
	10.1.2	Gestión de cambios	AI6.1 Estándares y procedimientos para cambios AI6.2 Evaluación de impacto, priorización y autorización AI6.3 Cambios de emergencia AI6.4 Seguimiento y reportes de estado de los cambios AI6.5 Cierre y documentación del cambio
	10.1.3	Segregación de funciones	PO4.11 Segregación de funciones DS5.4 Gestión de cuentas de usuario
	10.1.4	Separación de los entornos de desarrollo, pruebas y Producción	PO4.11 Segregación de funciones AI3.4 Ambiente de prueba de factibilidad AI7.4 Ambiente de pruebas
10.2	Gestión de la entrega de servicios de terceros		-
	10.2.1	Entrega de servicios	DS1.1 Marco de trabajo para la gestión de niveles de servicio DS1.2 Definición de servicios DS1.3 Acuerdos de niveles de servicio DS2.4 Monitoreo del desempeño de proveedores
	10.2.2	Monitoreo y revisión de los servicios de terceros	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio DS2.4 Monitoreo del desempeño de proveedores ME2.6 Control interno para terceros
	10.2.3	Gestión de cambios a los servicios de terceros	DS1.5 Monitoreo y reporte del cumplimiento de los niveles de servicio DS2.2 Gestión de relaciones con proveedores DS2.3 Gestión de riesgos de proveedores
10.3	Planeamiento y aceptación de sistemas		-
	10.3.1	Gestión de la capacidad	DS3.1 Planeación del desempeño y la capacidad DS3.2 Capacidad y desempeño actual DS3.3 Capacidad y desempeño futuros

	10.3.2	Aceptación del sistema	PO3.4 Estándares tecnológicos AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio AI1.4 Requerimientos, decisión de factibilidad y aprobación AI2.4 Seguridad y disponibilidad de las aplicaciones AI2.8 Aseguramiento de la calidad del software AI4.4 Transferencia de conocimiento al personal de operaciones y soporte AI7.7 Pruebas de aceptación final
10.4	Protección contra código móvil y malicioso		-
	10.4.1	Controles contra código malicioso	DS5.9 Prevención, detección y corrección de Software malicioso
	10.4.2	Controles contra código móvil	DS5.9 Prevención, detección y corrección de Software malicioso
10.5	Respaldos		-
	10.5.1	Respaldo de la información	DS4.9 Almacenamiento externo de respaldos DS11.2 Acuerdos para el almacenamiento y la conservación DS11.5 Respaldo y restauración DS11.6 Requisitos de seguridad para la gestión de datos
10.6	Gestión de la seguridad de redes		
	10.6.1	Controles de red	PO4.11 Segregación de funciones DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
	10.6.2	Seguridad de los servicios de red	DS5.7 Protección de la tecnología de seguridad DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
10.7	Manejo de medios de almacenamiento		-
	10.7.1	Gestión de medios removibles de almacenamiento	PO2.3 Esquema de clasificación de datos DS11.2 Acuerdos para el almacenamiento y la conservación DS11.3 Sistema de gestión de la librería de medios DS11.4 Desechar
	10.7.2	Eliminación de medios de almacenamiento	DS11.3 Sistema de gestión de la librería de medios DS11.4 Desechar
	10.7.3	Procedimientos para el manejo de la información	PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI DS11.6 Requisitos de seguridad para la gestión de datos
	10.7.4	Seguridad de la documentación de sistemas	AI4.4 Transferencia de conocimiento al personal de operaciones y soporte DS5.7 Protección de la tecnología de seguridad DS9.2 Identificación y mantenimiento de elementos de la configuración DS9.3 Revisión de integridad de la configuración DS13.1 Procedimientos e instrucciones de operación
10.8	Intercambio de información		-
	10.8.1	Políticas y procedimientos para el intercambio de información	PO2.3 Esquema de clasificación de datos PO6.2 Riesgo corporativo y marco de referencia para el control interno de TI DS11.1 Requerimientos del negocio para la gestión de los datos
	10.8.2	Acuerdos de intercambio	PO2.3 Esquema de clasificación de datos PO3.4 Estándares tecnológicos AI5.2 Gestión de contratos con proveedores DS2.3 Gestión de riesgos de proveedores
	10.8.3	Medios de almacenamiento físico en tránsito	DS11.6 Requisitos de seguridad para la gestión de datos
	10.8.4	Mensajería electrónica	DS5.8 Gestión de llaves criptográficas DS11.6 Requisitos de seguridad para la gestión de datos
	10.8.5	Sistemas de información del negocio	DS11.6 Requisitos de seguridad para la gestión de datos
10.9	Servicios de comercio electrónico		-
	10.9.1	Comercio electrónico	AC4 Integridad y validez del procesamiento AC6 Autenticación e integridad de transacciones DS5.11 Intercambio de datos sensitivos
	10.9.2	Transacciones en línea	AC3 Verificaciones de exactitud, totalidad, y autenticidad AC4 Integridad y validez del procesamiento AC5 Revisión de salidas, reconciliación y manejo de errores AC6 Autenticación e integridad de transacciones
	10.9.3	Información de dominio público	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI
10.10	Monitoreo		-
	10.10.1	Logs de auditoría	AI2.3 Control y auditabilidad de las aplicaciones DS5.7 Protección de la tecnología de seguridad

	10.10.2	Monitoreo del uso de los sistemas	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad ME1.2 Definición y recolección de los datos de monitoreo ME2.2 Revisiones de supervisión ME2.5 Aseguramiento del control interno ME4.7 Aseguramiento independiente
	10.10.3	Protección de logs	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad DS5.7 Protección de la tecnología de seguridad
	10.10.4	Logs de administrador y de operador	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad DS5.7 Protección de la tecnología de seguridad ME2.2 Revisiones de supervisión ME2.5 Aseguramiento del control interno
	10.10.5	Logs de errores	AI2.3 Control y auditabilidad de las aplicaciones DS5.7 Protección de la tecnología de seguridad
	10.10.6	Sincronización de relojes	DS5.7 Protección de la tecnología de seguridad
11.0 CONTROL DE ACCESO			-
11.1	Requisitos del negocio para el control de acceso		-
	11.1.1	Políticas de control de acceso	PO2.2 Diccionario de datos empresarial y reglas de sintaxis de los datos PO2.3 Esquema de clasificación de datos PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad DS5.4 Gestión de cuentas de usuario
11.2	Gestión de accesos de usuarios		-
	11.2.1	Registro de usuarios	DS5.4 Gestión de cuentas de usuario
	11.2.2	Gestión de privilegios	DS5.4 Gestión de cuentas de usuario
	11.2.3	Gestión de contraseñas de usuarios	DS5.3 Gestión de identidad
	11.2.4	Revisión de derechos de acceso de usuarios	DS5.4 Gestión de cuentas de usuario
11.3	Responsabilidades de usuario		-
	11.3.1	Uso de contraseñas	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS5.4 Gestión de cuentas de usuario
	11.3.2	Equipos desatendidos de usuario	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS5.7 Protección de la tecnología de seguridad
	11.3.3	Políticas de escritorios y pantallas limpias	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS5.7 Protección de la tecnología de seguridad
11.4	Control de acceso a la red		-
	11.4.1	Políticas de uso de los servicios de red	DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
	11.4.2	Autenticación de usuario para conexiones Externas	DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
	11.4.3	identificación de equipos en redes	DS5.7 Protección de la tecnología de seguridad DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos DS9.2 Identificación y mantenimiento de elementos de la configuración
	11.4.4	Protección de puertos de configuración y diagnóstico remoto	DS5.7 Protección de la tecnología de seguridad DS5.9 Prevención, detección y corrección de Software malicioso DS 5.11 Exchange of sensitive data
	11.4.5	Segregación en redes	DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
	11.4.6	Control de conexiones en la red	DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
	11.4.7	Control de enrutamiento en la red	DS5.9 Prevención, detección y corrección de Software malicioso DS5.11 Intercambio de datos sensitivos
11.5	Control de acceso al sistema operativo		-

	11.5.1	Procedimientos seguros de inicio de sesión	DS5.4 Gestión de cuentas de usuario DS5.7 Protección de la tecnología de seguridad
	11.5.2	Identificación y autenticación de usuario	DS5.3 Gestión de identidad
	11.5.3	Sistema de gestión de contraseñas	DS5.4 Gestión de cuentas de usuario
	11.5.4	Uso de utilitarios del sistema	AI6.3 Cambios de emergencia DS5.7 Protección de la tecnología de seguridad
	11.5.5	Período de inactividad de sesión	DS5.7 Protección de la tecnología de seguridad
	11.5.6	Limitación del tiempo de conexión	DS5.7 Protección de la tecnología de seguridad
11.6	Control de acceso a la información y a la aplicación		-
	11.6.1	Restricción de acceso a la información	DS5.4 Gestión de cuentas de usuario
	11.6.2	Aislamiento de sistemas sensitivos	AI1.2 Reporte de análisis de riesgos AI2.4 Seguridad y disponibilidad de las aplicaciones DS5.7 Protección de la tecnología de seguridad DS5.10 Seguridad de la red DS5.11 Intercambio de datos sensitivos
11.7	Computación móvil y teletrabajo		
	11.7.1	Computación móvil y las comunicaciones	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad DS5.7 Protección de la tecnología de seguridad
	11.7.2	Teletrabajo	PO3.4 Estándares tecnológicos PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS5.2 Plan de seguridad de TI DS5.3 Gestión de identidad DS5.7 Protección de la tecnología de seguridad
12.0 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN			-
12.1	Requisitos de seguridad de los sistemas de información		-
	12.1.1	Análisis y especificación de requisitos de seguridad	AI1.2 Reporte de análisis de riesgos AI2.4 Seguridad y disponibilidad de las aplicaciones AI3.2 Protección y disponibilidad de la infraestructura
12.2	Procesamiento correcto en aplicaciones		-
	12.2.1	Validación de datos de entrada	AI2.3 Control y auditabilidad de las aplicaciones
	12.2.2	Control de procesamiento interno	AI2.3 Control y auditabilidad de las aplicaciones
	12.2.3	Integridad de mensajes	AI2.3 Control y auditabilidad de las aplicaciones AI2.4 Seguridad y disponibilidad de las aplicaciones DS5.8 Gestión de llaves criptográficas
	12.2.4	Validación de datos de salida	AI2.3 Control y auditabilidad de las aplicaciones
12.3	Controles criptográficos		-
	12.3.1	Políticas de uso de controles criptográficos	PO6.2 Riesgo corporativo y marco de referencia del control interno de TI AI2.4 Seguridad y disponibilidad de las aplicaciones DS5.8 Gestión de llaves criptográficas
	12.3.2	Gestión de claves	DS5.8 Gestión de llaves criptográficas
12.4	Seguridad de archivos del sistema		-
	12.4.1	Control del software de operaciones	DS5.7 Protección de la tecnología de seguridad DS9.1 Repositorio y línea base de configuración
	12.4.2	Protección de los datos de prueba de sistema	AI3.3 Mantenimiento de la infraestructura DS2.4 Monitoreo del desempeño de proveedores DS9.1 Repositorio y línea base de configuración DS9.2 Identificación y mantenimiento de elementos de la configuración DS11.6 Requisitos de seguridad para la gestión de datos
	12.4.3	Control de acceso al código fuente de los programas	AI2.4 Seguridad y disponibilidad de las aplicaciones AI7.4 Ambiente de pruebas AI7.6 Pruebas de cambios DS11.3 Sistema de gestión de la librería de medios DS11.6 Requisitos de seguridad para la gestión de datos
12.5	12.5.1	Procedimientos de control de cambios	AI2.6 Actualizaciones importantes en sistemas existentes AI6.2 Evaluación de impacto, priorización y autorización AI6.3 Cambios de emergencia AI7.2 Plan de pruebas
	12.5.2	Revisión técnica de las aplicaciones luego de cambios en el sistema operativo	AI2.4 Seguridad y disponibilidad de las aplicaciones AI3.3 Mantenimiento de la infraestructura AI7.2 Plan de pruebas AI7.4 Ambiente de pruebas AI7.6 Pruebas de cambios AI7.7 Pruebas de aceptación final DS9.3 Revisión de integridad de la configuración

	12.5.3	Restricciones en los cambios a los paquetes de software	AI2.5 Configuración e implementación de software de aplicación adquirido AI6.1 Estándares y procedimientos para cambios AI6.2 Evaluación de impacto, priorización y autorización AI6.3 Cambios de emergencia DS9.2 Identificación y mantenimiento de elementos de la configuración
	12.5.4	Fuga de información	AI2.4 Seguridad y disponibilidad de las aplicaciones AI7.7 Pruebas de aceptación final
	12.5.5	Outsourcing de desarrollo de software	PO8.3 Estándares para desarrollos y adquisiciones AI2.7 Desarrollo de software aplicativo AI5.2 Gestión de contratos con proveedores DS2.4 Monitoreo del desempeño de proveedores
12.6	Gestión de vulnerabilidades técnicas		-
	12.6.1	Control de vulnerabilidades técnicas	AI3.3 Mantenimiento de la infraestructura AI6.2 Evaluación de impacto, priorización y autorización AI6.3 Cambios de emergencia DS5.5 Pruebas, vigilancia y monitoreo de la seguridad DS5.7 Protección de la tecnología de seguridad DS9.2 Identificación y mantenimiento de elementos de la configuración
13.0 GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN			-
13.1	Reporte de debilidades y eventos de seguridad de información		-
	13.1.1	Reporte de eventos de seguridad de información	PO9.3 Identificación de eventos DS5.6 Definición de incidente de seguridad DS8.2 Registro de consultas de clientes
	13.1.2	Reporte de debilidades de seguridad de información	PO9.3 Identificación de eventos DS5.5 Pruebas, vigilancia y monitoreo de la seguridad DS5.6 Definición de incidente de seguridad DS5.7 Protección de la tecnología de seguridad DS8.2 Registro de consultas de clientes DS8.3 Escalamiento de incidentes
13.2	Gestión y mejora de incidentes de seguridad de información		-
	13.2.1	Responsabilidades y procedimientos	PO6.1 Política y entorno de control de TI DS5.6 Definición de incidente de seguridad DS8.2 Registro de consultas de clientes
	13.2.2	Aprendiendo de los incidentes de seguridad de información	PO5.4 Gestión de costos de TI AI4.4 Transferencia de conocimiento al personal de operaciones y soporte DS8.4 Cierre de incidentes DS8.5 Reportes y análisis de tendencias DS10.1 Identificación y clasificación de problemas DS10.2 Seguimiento y resolución de problemas
	13.2.3	Recolección de evidencia	AI2.3 Control y auditabilidad de las aplicaciones DS5.6 Definición de incidente de seguridad DS5.7 Protección de la tecnología de seguridad DS8.2 Registro de consultas de clientes DS8.3 Escalamiento de incidentes DS8.4 Cierre de incidentes
14.0 GESTIÓN DE CONTINUIDAD DE NEGOCIOS			-
14.1	**Inclusión de SI en el proceso BCP**		-
	14.1.1	Incluir seguridad de información en el proceso de gestión BCP	PO3.1 Planeamiento de la orientación tecnológica PO9.1 Marco de trabajo de gestión de riesgos PO9.2 Establecimiento del contexto del riesgo DS4.1 Marco de trabajo de continuidad de TI DS4.3 Recursos críticos de TI DS4.8 Recuperación y reanudación de los servicios de TI DS8.3 Escalamiento de incidentes
	14.1.2	Continuidad del negocio y evaluación de riesgos	PO9.1 Marco de trabajo de gestión de riesgos PO9.2 Establecimiento del contexto del riesgo PO9.4 Evaluación de riesgos de TI DS4.1 Marco de trabajo de continuidad de TI DS4.3 Recursos críticos de TI
	14.1.3	Inclusión de SI en el desarrollo e implementación de planes de continuidad	DS4.2 Planes de continuidad de TI DS4.8 Recuperación y reanudación de los servicios de TI
	14.1.4	Marco de trabajo de BCP	DS4.1 Marco de trabajo de continuidad de TI DS8.1 Mesa de servicios DS8.3 Escalamiento de incidentes
	14.1.5	Pruebas, mantenimiento y reevaluación del BCP	PO3.1 Planeamiento de la orientación tecnológica DS4.4 Mantenimiento del plan de continuidad de TI DS4.5 Pruebas del plan de continuidad de TI DS4.6 Entrenamiento en el plan de continuidad de TI DS4.7 Distribución del plan de continuidad de TI DS4.10 Revisión postreanudación

15.0 CUMPLIMIENTO			-
15.1	Cumplimiento de requisitos legales		-
	15.1.1	Identificación de legislación aplicable	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual
	15.1.2	Derechos de propiedad intelectual	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento
	15.1.3	Protección de registros organizacionales	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento DS11.2 Acuerdos para el almacenamiento y la conservación
	15.1.4	Protección de datos y privacidad de la información personal	PO4.6 Establecer roles y responsabilidades PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento DS2.2 Gestión de relaciones con proveedores ME3.1 Identificación de los requisitos legales, regulatorios y de cumplimiento contractual ME3.3 Evaluación del cumplimiento con requerimientos externos ME3.4 Aseguramiento positivo del cumplimiento
	15.1.5	Prevención del uso indebido de instalaciones de procesamiento de información	PO4.14 Políticas y procedimientos para el personal contratado PO6.2 Riesgo corporativo y marco de referencia del control interno de TI DS9.2 Identificación y mantenimiento de elementos de la configuración DS9.3 Revisión de integridad de la configuración
	15.1.6	Regulación de controles criptográficos	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento DS5.8 Gestión de llaves criptográficas
15.2	Cumplimientos técnicos, de estándares y de políticas de seguridad		-
	15.2.1	Cumplimiento con políticas y estándares de seguridad	PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento PO6.2 Riesgo corporativo y marco de referencia del control interno de TI ME2.1 Monitoreo del marco de trabajo de control interno ME2.2 Revisiones de supervisión ME2.3 Excepciones de control ME2.4 Autoevaluación de control ME2.5 Aseguramiento del control interno ME2.6 Control interno para terceros ME2.7 Acciones correctivas
	15.2.2	Verificación de cumplimiento técnico	DS5.5 Pruebas, vigilancia y monitoreo de la seguridad DS5.7 Protección de la tecnología de seguridad ME2.5 Aseguramiento del control interno
15.3	Consideraciones de auditoría de sistemas de información		-
	15.3.1	Controles de auditoría de sistemas de información	AI2.3 Control y auditabilidad de las aplicaciones DS5.5 Pruebas, vigilancia y monitoreo de la seguridad ME2.5 Aseguramiento del control interno
	15.3.2	Protección de herramientas de auditoría de sistemas de información	AI2.3 Control y auditabilidad de las aplicaciones AI2.4 Seguridad y disponibilidad de las aplicaciones DS5.7 Protección de la tecnología de seguridad

Fuente: Cobit 4.1

Resumen del Capítulo 2

En el presente Capítulo se ha detallado y explicado las diversas actividades que incluyen la metodología de auditoría de sistemas informáticos en entidades del Sistema Nacional de Control Peruano, la cual permite guiar a los auditores gubernamentales en las auditorías de sistemas informáticos que se realizan en entidades del sector público peruano.

La propuesta metodológica incluyó los roles y responsabilidades del personal que forma parte de las Comisiones de Auditorías (Jefe del Órgano de Control Institucional, Supervisor, Auditor Encargado y Auditores) permitiendo de esta manera, una mejor comunicación y coordinación entre cada uno de ellos.

Asimismo, la metodología propuesta ha sido estructurada en (3) tres etapas consecutivas (Planificación, Ejecución y Elaboración de Informe de Auditoría), cada una de ellas organizada en (3) pasos: “SE INICIA CON”, “CONTINUA CON” y “FINALIZA CON”, con el fin de facilitar su uso; especificándose los diversos documentos que se emiten en cada una de dichas etapas.

Por último, la propuesta metodológica hace referencia a los marcos de referencia COSO, COBIT e ISO/IEC 27002 con el fin que se puedan identificar controles y riesgos asociados a los procesos de la entidad que se está auditando.

Capítulo 3

Aplicación y Validación de la Propuesta Metodológica que permite guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos del Sector Público Peruano

El presente capítulo trata sobre el uso de la metodología propuesta en el Capítulo 2 del presente trabajo de tesis aplicado en la Oficina de Control Interno de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), específicamente en la División de Auditoría de Sistemas Informáticos.

Es de significar que la Oficina de Control Interno de la SUNAT en su calidad de órgano de control institucional forma parte del Sistema Nacional de Control Peruano, el cual depende funcionalmente de la Contraloría General de la República y administrativamente de la SUNAT. La dependencia es funcional debido a que la Contraloría General dirige la labor operativa de los órganos de control institucional. Asimismo, la dependencia es administrativa debido a que la SUNAT asigna los recursos necesarios (infraestructura, logísticos y humanos) para el cumplimiento de las funciones encomendadas.

Sobre el particular, en concordancia al principio de autocontrol establecido en las Normas de Control Interno[7], aplicable a las entidades del Estado; el suscrito aplicó la propuesta metodológica como parte del autocontrol que cada funcionario ó servidor público debe realizar en su propio trabajo, con el fin de efectuar correctivos para el mejoramiento de las labores asignadas.

---

[7] *Aprobado mediante Resolución de Contraloría N° 320-2006-CG, publicado el 03.NOV.2006.*

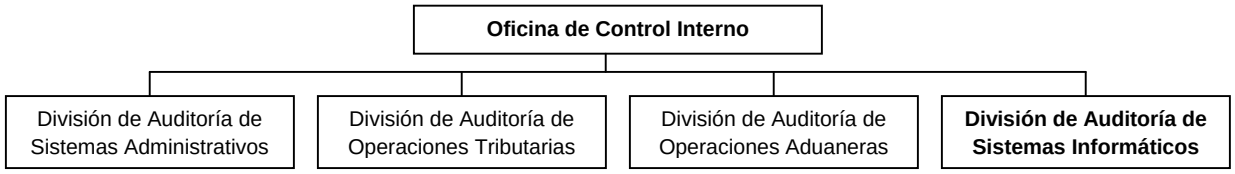
3.1. Antecedentes

Desde setiembre del año 2004, el suscrito viene trabajando como auditor gubernamental en la División de Auditoría de Sistemas Informáticos de la Oficina de Control Interno de la Superintendencia Nacional de Aduanas y de Administración Tributaria (SUNAT), luego de haber ganado un concurso interno para cubrir una plaza vacante en dicha unidad organizacional.

Asimismo, según el Reglamento de Organización y Funciones de la SUNAT[8], la Oficina de Control Interno es el órgano encargado de cautelar la correcta administración de recursos de la institución y la confiabilidad de su información financiera, mediante el control posterior de la gestión contable, financiera y administrativa, así como verificar la debida aplicación de las normas, procedimientos y técnicas de la institución, en armonía con las disposiciones del Sistema Nacional de Control y demás normas vigentes.

Dicho órgano de control institucional está conformado por cuatro (4) divisiones, tal como se muestra en el siguiente gráfico:

Gráfico N° 3.1. **Organigrama de la Oficina de Control Interno de SUNAT**



Al respecto, la División de Auditoría de Sistemas Informáticos se encarga[9] de ejecutar las acciones de control en las unidades organizacionales de la SUNAT relacionados a aspectos de carácter informático.

Sobre el particular, en el periodo del año 2004 al 2012, el suscrito ha participado en aproximadamente treinta (30) auditorías gubernamentales (concluidas). De las cuales, en trece (13) he participado como Auditor Encargado y en diecisiete (17) he participado en calidad de Auditor, tal como se aprecia a continuación:

---

[8] *Aprobado mediante Decreto Supremo N° 115-2002-PCM, publicado el 28.OCT.2002.*

[9] *Aprobado mediante Resolución de Superintendencia N° 190-2002/SUNAT del 31.DIC.2002.*

Gráfico N° 3.2. **Cantidad de Auditorías por Año**

Año	Auditor Encargado	Auditor	Total
2004	0	2	2
2005	1	2	3
2006	4	1	5
2007	1	1	2
2008	2	1	3
2009	0	2	2
2010	2	5	7
2011	1	1	2
2012	2	2	4
	13	**17**	**30**

3.2. Aplicación de la Propuesta Metodológica

Del total de treinta (30) auditorías gubernamentales realizadas entre el año 2004 al 2012 en las cuales el suscrito participó en calidad de Auditor Encargado o Auditor de las Comisiones de Auditoría que se conformaron en dichos años; se precisa que para los años 2011 y 2012 el suscrito aplicó la propuesta metodológica a seis (6) auditorías gubernamentales: tres (3) correspondientes a auditorías en las que estuve designado como Auditor Encargado y tres (3) auditorías como Auditor.

Al respecto, cuando el suscrito estuvo designado como Auditor Encargado en las auditorías gubernamentales de sistemas informáticos realizadas entre los años 2011 y 2012, la propuesta metodológica se aplicó a todas las etapas de la auditoría gubernamental (Planificación, Ejecución y Elaboración del Informe de Auditoría). Asimismo, cuando el suscrito estuvo designado como Auditor, la metodología sólo se aplicó en la etapa de Ejecución, tal como se aprecia a continuación:

Gráfico N° 3.3. **Número de Auditorías aplicadas con la propuesta metodológica**

Año	Auditor Encargado	Etapas de la Auditoría Gubernamental	Auditor	Etapas de la Auditoría Gubernamental
2011	1	Planificación Ejecución Elaboración de Informe	1	Ejecución
2012	2		2	
	3		**3**	
Total: 6 auditorías gubernamentales				

3.3. Validación de la Propuesta Metodológica

Considerando que la metodología propuesta establece las actividades que tiene que realizar cada una de las personas integrantes de las Comisiones de Auditoría (Jefe del Órgano de Control Institucional, Supervisor, Auditor Encargado y Auditores), se precisa que la validación de la propuesta metodológica se ha realizado en las etapas de auditoría en las cuales el suscrito participó como Auditor Encargado ó Auditor correspondiente a las seis (6) auditorías de sistemas informáticos realizadas entre los años 2011 y 2012 detalladas en el Gráfico N° 3.3.

En ese sentido, debido al carácter confidencial de la información a las que tienen acceso las Comisiones de Auditoría durante las auditorías gubernamentales y de las cuales se tiene que mantener reserva aún hasta cuando se culmine con el vínculo laboral, se procederá a detallar en forma general las actividades más importantes realizadas durante las etapas que comprende la auditoría gubernamental (Planificación, Ejecución y Elaboración de Informe de Auditoría) con el fin de poder validar la propuesta metodológica, tal como se detalla a continuación:

3.3.1. Etapa de Planificación

La etapa de Planificación incluye la aplicación de las siguientes Normas de Auditoría Gubernamental:

- NAGU 2.10: Planificación General.
- NAGU 2.20: Planificación Específica.
- NAGU 2.30: Programa de Auditoría.
- NAGU 2.40: Archivo Permanente.

Al respecto, considerando que dichas Normas de Auditoría forman parte de la aplicación de la metodología propuesta, se procede a indicar de qué manera las actividades plasmadas en la metodología contribuyeron al cumplimiento de las auditorías de sistemas informáticos realizadas en los años 2011 y 2012:

a. Desde el punto de vista de la Simplicidad:

El uso de la propuesta metodológica permitió efectuar en forma simple las actividades a realizar en las auditorías de sistemas informáticos relacionadas a la Planificación General, Planificación Específica, Programa de Auditoría y Archivo Permanente; las cuales están interrelacionadas y apuntan a un mismo objetivo que es la elaboración del Plan y Programa de Auditoría.

b. Desde el punto de vista del Orden:

Al haber tenido claro las actividades a realizar relacionadas a las NAGUS 2.10, 2.20, 2.30 y 2.40 se pudo efectuar ordenadamente las actividades contenidas en la propuesta metodológica.

En este punto, es de resaltar que llevar un orden pre-establecido desde el principio de la auditoría gubernamental permitió contar con información ordenada y actualizada correspondiente al Archivo Permanente, el cual está sustentado en la normativa interna y externa aplicable a la SUNAT, documentación de auditorías anteriores relacionadas a los temas que se estuvieron auditando así como de documentación relacionada a las tecnologías de información de los sistemas informáticos; permitiendo de esta manera una consulta más rápida de dicha documentación.

Dicho Archivo Permanente permitió dar sustento a la normativa referenciada en cada uno de los documentos que emitió la Comisión de Auditoría durante cada una de las fases que conforman la auditoría gubernamental.

c. Desde el punto de vista de la Eficiencia:

Al haberse efectuado ordenadamente las actividades relacionadas a las NAGUS 2.10, 2.20, 2.30 y 2.40 se pudo realizar eficientemente las actividades contenidas en la propuesta metodológica.

Dicha eficiencia, permitió seleccionar mejor las auditorías de sistemas informáticos que fueron incluidas en el Plan Anual de Control, las cuales están dirigidas a contribuir al logro de los objetivos y metas institucionales.

Asimismo, al tener claro las fechas aproximadas de elaboración del Plan Anual de Control (últimos meses del año), se pudo aportar mejores ideas relacionadas a auditorías de sistemas informáticos, que fueron incluidas en la elaboración del Plan Anual de Control, considerando la experiencia que se tiene respecto de la entidad así como de auditorías realizadas anteriormente.

Del mismo modo, mediante la aplicación de las Normas de Control Interno (basadas en el marco de referencia COSO) para la identificación preliminar de controles y riesgos, se obtuvo Planes y Programas de Auditoría que enfocaron de manera más eficiente los objetivos generales, objetivos específicos así como los procedimientos mínimos a realizar en las auditorías de sistemas informáticos.

d. Desde el punto de vista del Cumplimiento de Plazos:

No existió variación respecto del cumplimiento para la remisión del Proyecto del Plan Anual de Control a la Contraloría General de la República, ya que son plazos previamente establecidos, los cuales tienen que ser debidamente cumplidos.

Sin embargo, la propuesta metodológica contribuyó al cumplimiento del cronograma establecido en los Planes y Programas de Auditoría correspondiente a la etapa de Planificación.

En ese sentido, se resume en términos generales el grado de beneficios alcanzados con la metodología propuesta, correspondiente a los años 2011 y 2012, relacionados a las NAGU 2.10, 2.20, 2.30 y 2.40:

- ✓ Simplicidad : Mayor
- ✓ Orden : Mayor
- ✓ Eficiencia : Mayor
- ✓ Cumplimiento de Plazos : Mayor

3.3.2. Etapa de Ejecución

La etapa de Ejecución incluye la aplicación de las siguientes Normas de Auditoría Gubernamental:

- NAGU 3.10: Evaluación de la Estructura de Control Interno.
- NAGU 3.20: Evaluación del cumplimiento de disposiciones Legales y Reglamentarias.
- NAGU 3.30: Supervisión del trabajo de auditoría.
- NAGU 3.40: Evidencia suficiente, competente y relevante.
- NAGU 3.50: Papeles de trabajo.
- NAGU 3.60: Comunicación de hallazgos.
- NAGU 3.70: Carta de representación.

Al respecto, considerando que dichas Normas de Auditoría forman parte de la aplicación de la metodología propuesta, se procede a indicar de qué manera las actividades plasmadas en la metodología contribuyeron al cumplimiento de las auditorías de sistemas informáticos realizadas en los años 2011 y 2012:

a. Desde el punto de vista de la Simplicidad:

El uso de la propuesta metodológica permitió realizar en forma simple las actividades relacionadas al cumplimiento de las normas de auditoría gubernamental; las cuales están interrelacionadas y apuntan a un mismo

objetivo que es la culminación del trabajo de campo de las auditorías gubernamentales enfocadas a los sistemas informáticos.

b. Desde el punto de vista del Orden:

Al tener claro las actividades a realizar respecto de Evaluación de la Estructura de Control Interno, Evaluación del cumplimiento de disposiciones legales y reglamentarias, Supervisión del trabajo de auditoría, Evidencia suficiente, competente y relevante, Papeles de trabajo, Comunicación de hallazgos y Carta de representación se pudo realizar ordenadamente las actividades contenidas en la propuesta metodológica.

En este punto, es de resaltar que llevar un orden pre-establecido durante la ejecución de la auditoría gubernamental contribuyó a que se puedan efectuar las actividades relacionadas al cumplimiento de la evaluación de la estructura de control interno de las tecnologías de información que incluyó la respectiva evaluación de los riesgos asociados a las tecnologías de información de los sistemas informáticos que se auditaron (desde el punto de vista de la confidencialidad, integridad y disponibilidad de la información) así como, la evaluación del cumplimiento de normativa interna y externa aplicable a SUNAT.

c. Desde el punto de vista de la Eficiencia:

Al haberse efectuado ordenadamente las actividades relacionadas al cumplimiento de las normas de auditoría gubernamental se pudo realizar eficientemente las actividades contenidas en la propuesta metodológica.

Dicha eficiencia, contribuyó a realizar una evaluación eficiente de los controles generales y detallados de las tecnologías de información correspondientes a los sistemas informáticos que se estuvieron auditando, utilizando para ello los estándares internacionales COBIT 4.1 e ISO/IEC 27002.

En ese sentido, el trabajo proporcionado por los auditores producto del trabajo de campo realizado, se encuentra debidamente evidenciado en los papeles de trabajo.

d. Desde el punto de vista del Cumplimiento de Plazos:

La propuesta metodológica permitió el cumplimiento del cronograma establecido en los Planes y Programas de Auditoría correspondiente a la etapa de Ejecución de las auditorías gubernamentales enfocada a los sistemas informáticos.

En ese sentido, se resume en términos generales el grado de beneficios alcanzados con la metodología propuesta, correspondiente a los años 2011 y 2012, relacionados a las NAGU 3.10, 3.20, 3.30, 3.40, 3.50, 3.60 y 3.70:

- ✓ Simplicidad : Mayor
- ✓ Orden : Mayor
- ✓ Eficiencia : Mayor
- ✓ Cumplimiento de Plazos : Mayor

3.3.3. Etapa de Elaboración del Informe de Auditoría

La etapa de Elaboración del Informe de Auditoría incluye la aplicación de las siguientes Normas de Auditoría Gubernamental:

- NAGU 4.10: Elaboración del informe.
- NAGU 4.20: Oportunidad del informe
- NAGU 4.30: Características del informe.
- NAGU 4.40: Contenido del informe.
- NAGU 4.60: Seguimiento de recomendaciones de auditorías anteriores.

Asimismo, considerando que la metodología propuesta incluye actividades a realizar relacionadas a la NAGU 4.50 (Informe Especial) se precisa que para las auditorías de sistemas informáticos realizadas entre los años 2011 y 2012 y en las cuales participó el suscrito, no ameritaron la elaboración de Informes Especiales (NAGU 4.50) al no haberse identificado indicios de responsabilidad civil y/o penal.

En ese sentido, y en base a lo indicado en el párrafo precedente, se procede a indicar de qué manera las actividades plasmadas en la metodología propuesta contribuyeron al cumplimiento de las normas de auditoría gubernamental relacionadas a las auditorías de sistemas informáticos realizadas en los años 2011 y 2012:

a. Desde el punto de vista de la Simplicidad:

El uso de la propuesta metodológica permitió realizar en forma simple las actividades relacionadas a la Elaboración del informe, Oportunidad del informe, Características del informe, Contenido del informe, Informe Especial y Seguimiento de recomendaciones; las cuales están interrelacionadas y apuntan a un mismo objetivo que es la emisión final del informe de auditoría de sistemas informáticos.

b. Desde el punto de vista del Orden:

Al tener claro las actividades a realizar respecto de las NAGUS 4.10, 4.20, 4.30, 4.40, 4.50 y 4.60 se pudo realizar ordenadamente la ejecución de las actividades contenidas en la propuesta metodológica.

En este punto, es de resaltar que el haber llevado un orden pre-establecido durante la elaboración de los informes de auditorías gubernamental contribuyó a que se puedan realizar mejores informes producto de las auditorías de sistemas informáticos. Dichas mejoras, se vieron reflejadas en el contenido de dichos informes, al haber sido redactados en forma ordenada, constructiva, sencilla y entendible; habiéndose expuestos las situaciones identificadas en forma objetiva y exacta, los cuales están debidamente sustentados en sus respectivos papeles de trabajo.

c. Desde el punto de vista de la Eficiencia:

Al haberse efectuado ordenadamente las actividades relacionadas a las NAGUS 4.10, 4.20, 4.30, 4.40 y 4.60 se pudo realizar eficientemente la ejecución de las actividades contenidas en la propuesta metodológica.

Dicha eficiencia, se materializó en la calidad de las recomendaciones de los informes emitidos producto de las auditorías de sistemas informáticos realizados.

Al respecto, el titular de la SUNAT dispuso a las unidades organizaciones competentes la implementación de las recomendaciones contenidas en los informes de auditoría.

d. Desde el punto de vista del Cumplimiento de Plazos:

La propuesta metodológica permitió el cumplimiento del cronograma establecido en los Planes y Programas de Auditoría correspondiente a la etapa de Elaboración del Informe de Auditoría de las auditorías gubernamentales enfocada a los sistemas informáticos que se realizaron en SUNAT.

En ese sentido, se resume en términos generales el grado de beneficios alcanzados con la metodología propuesta, correspondiente a los años 2011 y 2012, relacionados a las NAGU 4.10, 4.20, 4.30, 4.40 y 4.60:

- ✓ Simplicidad : Mayor
- ✓ Orden : Mayor
- ✓ Eficiencia : Mayor
- ✓ Cumplimiento de Plazos : Mayor

En base a lo señalado en los párrafos precedentes, relacionados a la validación de la propuesta metodológica correspondiente a las tres (3) etapas de las auditorías de sistemas informáticos correspondiente a los años 2011 y 2012, es importante señalar que los artículos 28° y 33° del Reglamento de los Órganos de Control Institucional[10] establecen que la Contraloría General de la República ejerce supervisión permanente sobre los Órganos de Control Institucional, entre los cuales, se encuentra la Oficina de Control Interno de SUNAT.

Al respecto, dicha supervisión puede incluir la evaluación de los informes resultantes de las auditorías realizadas, es decir, los informes emitidos por los órganos de control institucional pueden ser revisados por la Contraloría General, la cual puede solicitar las aclaraciones que considere necesarias, e inclusive puede disponer su reformulación, cuando considere que su elaboración no se ha sujetado a la normativa vigente, dando las instrucciones respectivas para superar las deficiencias identificadas.

En ese sentido, el suscrito no ha recibido ninguna observación acerca de los informes en los cuales he participado en calidad de Auditor Encargado o Auditor; lo cual es una forma de validar y acreditar que la metodología propuesta cumple con las disposiciones que ha emitido la Contraloría General de la República.

[10] *Aprobado mediante Resolución de Contraloría General Nº 459-2008-CG, publicado el 30.OCT.2008.*

Resumen del Capítulo 3

En el presente Capítulo se ha tratado la aplicación y validación de la propuesta metodológica que permite guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos del Sector Público Peruano.

Al respecto, entre los años 2011 y 2012 la propuesta metodológica fue aplicada y validada en la División de Auditoría de Sistemas Informáticos de la Oficina de Control Interno de la SUNAT. Dicho órgano de control institucional, forma parte del Sistema Nacional de Control Peruano.

Sobre el particular, la metodología propuesta fue utilizada en seis (6) auditorías gubernamentales correspondiente a los años 2011 y 2012, en las cuales el suscrito participó como Auditor ó Auditor Encargado. En ese sentido, la metodología se aplicó y validó en cada una de las tres etapas que forman parte de la auditoría gubernamental de sistemas informáticos: Planificación, Ejecución y Elaboración del Informe de Auditoría; obteniéndose mejoras de simplicidad, orden, eficiencia y cumplimiento de plazos en las actividades que conforman dichas etapas.

Conclusiones

Respecto de la evaluación realizada al marco normativo aplicable al proceso de auditoría de sistemas informáticos del Sistema Nacional de Control Peruano en entidades del Sector Público Peruano, se concluye lo siguiente:

1. Se ha determinado el marco normativo peruano aplicable a la propuesta metodológica que permite guiar las auditorías de sistemas informáticos en entidades del sector público peruano, el cual incluye, entre otros, la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República, el Reglamento de los Órganos de Control Institucional, la Ley de Control Interno de las Entidades del Estado, Normas de Control Interno, Guía para la implementación del Sistema de Control Interno de las entidades del Estado, Normas de Auditoría Gubernamental y Manual de Auditoría Gubernamental. Asimismo, dentro de dicho marco normativo se encuentra la normativa emitida por el Congreso de la República, Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) y normativa propia aplicable para cada entidad pública.

2. Se ha identificado que la Guía para la implementación del Sistema de Control Interno de las entidades del estado emitida por la Contraloría General de la República establece que para poder establecer controles relacionados a las tecnologías de la información y comunicaciones debe tomarse en cuenta estándares o buenas prácticas internacionales, entre las cuales se encuentra COBIT e ISO/IEC 27002 que permita desarrollar un marco propio adaptable a la realidad de cada entidad perteneciente al sector público peruano. En ese sentido, considerando que la Contraloría General de la República no ha emitido normatividad explícita que permita guiar las auditorías de sistemas informáticos en entidades del sector público peruano, se hace necesario el uso de dichos estándares o buenas prácticas internacionales en las auditorías gubernamentales enfocadas a los sistemas informáticos, permitiendo de está manera evaluar controles que podrían ser utilizados en los procesos informáticos de las entidades públicas con el fin de minimizar riesgos que puedan afectar el logro de los objetivos y metas institucionales.

3. Se ha identificado que entidades del Estado Peruano aplican estándares internacionales en la elaboración de su propia normativa, tal es el caso, de las Normas de Control Interno emitidas por la Contraloría General de la República las cuales se basan en el marco de trabajo internacional COSO; asimismo, la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 emitida por la Presidencia del Consejo de Ministros relacionada al uso obligatorio de buenas prácticas para la gestión de la seguridad de la información se basa en el estándar internacional ISO/IEC 27002:2005. En ese sentido, la propuesta metodológica planteada en el presente trabajo de tesis, que permite guiar las auditorías de sistemas informáticos del Sistema Nacional de Control Peruano en el Sector Público Peruano, también ha considerado en su elaboración la aplicación de dichos estándares internacionales (COSO, ISO/IEC 27002:2005) así como de COBIT.

Respecto de la Propuesta metodológica que permite guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos del Sector Público Peruano, se concluye lo siguiente:

4. Se ha proporcionado una propuesta metodológica que permite guiar las auditorías de sistemas informáticos en el Sistema Nacional de Control Peruano de una manera sencilla y práctica, la cual está basada en las tres (03) etapas de la auditoría gubernamental (Planificación, Ejecución y Elaboración del Informe de Auditoría), en concordancia a las Normas de Auditoría Gubernamental emitidas por la Contraloría General de la República.

5. Se ha determinado que para poder hacer uso de la metodología propuesta, se debe tener conocimiento de la normativa emitida por la Contraloría General de la República, Oficina Nacional de Gobierno Electrónico e Informática, estándares internacionales COSO, COBIT e ISO/IEC 27002) así como normatividad propia emitida por la entidad que se está auditando, con el fin de tener una base adecuada que permita aplicar adecuadamente los temas abordados en la propuesta metodológica, ya que dicha normativa se aplica en cada una de las etapas de la auditoría gubernamental enfocada a los sistemas informáticos.

6. Se ha identificado los roles y responsabilidades de cada una de las personas que conforman las Comisiones de Auditoría, tales como, Jefe del Órgano de Control Institucional, Supervisor, Auditor Encargado y Auditores; las cuales tienen por objetivo llevar adelante las auditorías de sistemas informáticos que se realizan en entidades del Sector Público Peruano.

7. Se ha identificado cada uno de los documentos que deben ser emitidos por parte de las Comisiones de Auditoría durante cada una de las fases de la auditoría gubernamental, tales como, Archivo Permanente, Plan y Programa de Trabajo, Memorándum de Control Interno, Carta de Representación, Informe Final de Auditoría, Informe Especial de Auditoría y Papeles de Trabajo generados en cada una de las etapas de auditoría gubernamental enfocada a los sistemas informáticos.

8. Se ha determinado los tres tipos de responsabilidades (administrativa, civil y/o penal) en los que puede incurrir el personal de las entidades públicas, como consecuencia de los actos realizados producto de las funciones asignadas en sus respectivas unidades organizaciones, las cuales son identificados por la Comisiones de Auditoría como parte de del trabajo de campo realizado durante la ejecución de la auditoría gubernamental.

Respecto de la Aplicación y Validación de la Propuesta Metodológica que permite guiar a los auditores gubernamentales del Sistema Nacional de Control Peruano en las auditorías de sistemas informáticos del Sector Público Peruano, se concluye lo siguiente:

9. Se ha aplicado la propuesta metodológica en seis (6) auditorías de sistemas informáticos que se realizaron en la Oficina de Control Interno de SUNAT, entre los años 2011 y 2012; en las cuales el suscrito participó como Auditor o Auditor Encargado, evidenciándose de esta manera su aplicabilidad en dicho órgano de control institucional perteneciente al Sistema Nacional de Control Peruano.

10. Se ha aplicado la propuesta metodológica en cada una de las tres etapas que conforman la auditoría de sistemas informáticos (Planificación, Ejecución y Elaboración del Informe de Auditoría), evidenciándose mejoras en cada una de dichas etapas, tales como, simplicidad, orden, eficiencia y cumplimiento de plazos; contribuyendo de está manera al cumplimiento del Plan Anual de Control de la Oficina de Control Interno de SUNAT.

11. Se ha determinado que las seis (6) auditorías de sistemas informáticos realizadas entre los años 2011 y 2012, en las cuales se utilizó la propuesta metodológica cumplen con los lineamientos establecidos por parte de la Contraloría General de la República, al no haberse recibido ninguna observación por parte de la Oficina de Control Interno de SUNAT ni de la propia Contraloría General de la República; asegurándose de esta manera la calidad de las auditorías realizadas.

Bibliografía

a. Respecto de la Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República:

1. **Congreso de la República del Perú.** (2002). *Ley N° 27785 – Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República*. Publicado en el Diario Oficial El Peruano el 23 de julio del 2002.

2. **Congreso de la República del Perú.** (2004). *Ley 28396 – Ley que modifica el Art. 43° de la Ley N° 27785*. Publicado en el Diario Oficial El Peruano el 25 de noviembre del 2004.

3. **Congreso de la República del Perú.** (2004). *Ley 28422 – Ley que modifica el inciso "i" del Art. 22° de la Ley N° 27785*. Publicado en el Diario Oficial El Peruano el 17 de diciembre del 2004.

4. **Congreso de la República del Perú.** (2010). *Ley 29622 – Ley que modifica la Ley N° 27785 y amplía las facultades en el proceso para sancionar en materia de responsabilidad administrativa funcional*. Publicado en el Diario Oficial El Peruano el 07 de diciembre del 2010.

b. Respecto de la Ley de Control Interno de las Entidades del Estado:

5. **Congreso de la República del Perú.** (2006). *Ley 28716 – Ley de Control Interno de las Entidades del Estado*. Publicado en el Diario Oficial El Peruano el 18 de abril del 2006.

6. **Congreso de la República del Perú.** (2011). *Ley 29743 – Ley que modifica el Art. 10 de la Ley 28716, Ley de Control Interno de las entidades del Estado*. Publicado en el Diario Oficial El Peruano el 09 de julio del 2011.

c. Respecto del Reglamento de los Órganos de Control Institucional:

7. **Contraloría General de la República del Perú.** (2008). *RC N° 459-2008-CG – Contralor General autoriza aprobar Reglamento de los Órganos de Control Institucional*. Publicado en el Diario Oficial El Peruano el 30 de octubre del 2008.

8. **Contraloría General de la República del Perú.** (2010). *RC N° 99-2010-CG – Modifican el Reglamento de los Órganos de Control Institucional*. Publicado en el Diario Oficial El Peruano el 23 de abril del 2010.

d. Respecto de las Normas de Control Interno:

9. **Contraloría General de la República del Perú.** (2006). *RC N° 320-2006-CG - Aprueban las Normas de Control Interno*. Publicado en el Diario Oficial El Peruano el 03 de noviembre del 2006.

e. Respecto de las Normas de Auditoría Gubernamental:

10. **Contraloría General de la República del Perú.** (1995). *RC N° 162-95-CG - Aprueban las Normas de Auditoría Gubernamental*. Publicado en el Diario Oficial El Peruano el 26 de setiembre de 1995.

11. **Contraloría General de la República del Perú.** (1999). *RC N° 141-99-CG - Modifican Normas y Manual de Auditoria Gubernamental*. Publicado en el Diario Oficial El Peruano el 29 de noviembre de 1999.

12. **Contraloría General de la República del Perú.** (2000). *RC N° 259-2000-CG - Modifican Normas de Auditoría Gubernamental*. Publicado en el Diario Oficial El Peruano el 13 de diciembre del 2000.

13. **Contraloría General de la República del Perú.** (2002). *RC N° 12-2002-CG - Sustituyen texto de la Norma de Auditoría Gubernamental 4.50 - Informe Especial*. Publicado en el Diario Oficial El Peruano el 22 de enero del 2002.

14. **Contraloría General de la República del Perú.** (2002). *RC N° 89-2002-CG - Suspende obligación de remitir Informes Especiales al Comité de Calidad de la Contraloría General, dispuesta por la NAGU 4.50*. Publicado en el Diario Oficial El Peruano el 11 de mayo del 2002.

f. Respecto del Manual de Auditoría Gubernamental:

15. **Contraloría General de la República del Perú.** (1998). *RC N° 152-98-CG - Aprueba*

Manual de Auditoría Gubernamental, Guía de Planeamiento de Auditoría Gubernamental, Guía de Elaboración del Informe de Auditoría Gubernamental, Guía de Papeles de Trabajo. Publicado en el Diario Oficial El Peruano el 19 de diciembre de 1998.

16. **Contraloría General de la República del Perú.** (1999). *RC N° 141-99-CG - Modifican Normas y Manual de Auditoria Gubernamental*. Publicado en el Diario Oficial El Peruano el 29 de noviembre de 1999.

g. Respecto de la Implementación de Recomendaciones:

17. **Contraloría General de la República del Perú.** (1999). *RC N° 279-2000-CG - Aprueban Directiva N° 14-2000-CG/B150 - Directiva para la Verificación y Seguimiento de implementación de recomendaciones derivadas de Informes de Acciones de Control*. Publicado en el Diario Oficial El Peruano el 30 de diciembre del 2000.

h. Respecto de la NTP ISO-IEC/17799-2007:

18. **Presidencia del Consejo de Ministros del Perú.** (1999). *RM N° 246-2007-PCM - Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI Tecnología 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*. Publicado en el Diario Oficial El Peruano el 25 de agosto del 2007.

i. Páginas WEB:

19. **Portal del Estado Peruano.** (2012). *Organización del Estado Peruano*. En Internet. Accesible en www.peru.gob.pe.

20. **Portal del Congreso de la República del Perú.** (2012). *Archivo digital de la Legislación del Perú (leyes, decretos ley, resoluciones legislativas, decretos legislativos y decretos de urgencia)*. En Internet. Accesible en www.congreso.gob.pe.

21. **Portal del Diario Oficial El Peruano.** (2012). *Normas Legales publicadas por las diversas entidades del Estado Peruano*. En Internet. Accesible en www.elperuano.pe.

22. **Portal de la Oficina Nacional de Gobierno Electrónico e Informática**. (2012). *Normatividad relacionada a temas informáticos, seguridad de la información, tecnologías de información y Comunicación (TIC)*. En Internet. Accesible en www.ongei.gob.pe.

23. **Portal del Committee of Sponsoring Organizations of the Treadway Commission**. (2012). *Marcos de trabajo y guías relacionadas a temas de control interno y riesgos.* En Internet. Accesible en http://www.coso.org/

24. **Portal de la Asociación de Auditoría y Control de Sistemas de Información - ISACA** (2012). *Objetivos de Control en Tecnologías de Información - COBIT. En Internet.* Accesible en http://www.isaca.org

25. **Portal de la International Organization for Standardization.** (2012). *Estándares internacionales relacionados a la gestión y buenas prácticas de la seguridad de la información.* En Internet. Accesible en www.iso.org

26. **Portal de la International Electrotechnical Commission**. (2012). *Estándares internacionales relacionados a temas eléctricos y electrónicos y tecnologías relacionadas*. En Internet. Accesible en www.iec.ch

ANEXOS DEL TRABAJO DE TESIS

Anexo N° 1
Marco Legal emitido por el Congreso Peruano relacionado al Sistema Nacional de Control Peruano

Objetivo: Identificar las leyes emitidas por el Congreso Peruano y que son de cumplimiento para las entidades pertenecientes al Sistema Nacional de Control Peruano.

Referenciado en: Página 48, correspondiente al numeral 1.1 del Capítulo 1 del presente trabajo de tesis.

A continuación, se detalla la normativa identificada para el presente trabajo de tesis:

Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República

	Ley N°	Fecha de Promulgación	Fecha de Publicación	Denominación
1	27785	22/07/2002	23/07/2002	Ley Orgánica del Sistema Nacional de Control y de la Contraloría General de la República.
2	28396	24/11/2004	25/11/2004	Ley que modifica el Art. 43° de la Ley N° 27785.
3	28422	16/12/2004	17/12/2004	Ley que modifica el inciso "i" del Art. 22° de la Ley N° 27785.
4	29622	06/12/2010	07/12/2010	Ley que modifica la Ley N° 27785 y amplía las facultades en el proceso para sancionar en materia de responsabilidad administrativa funcional.

Ley de Control Interno de las Entidades del Estado

	Ley N°	Fecha de Promulgación	Fecha de Publicación	Denominación
1	28716	17/04/2006	18/04/2006	Ley de Control Interno de las Entidades del Estado.
2	29743	30/06/2011	09/07/2011	Ley que modifica el Art. 10 de la Ley 28716, Ley de Control Interno de las entidades del Estado

Anexo N° 2
Marco Legal emitido por la Contraloría General de la República

Objetivo: Identificar las Resoluciones de Contraloría emitidas por la Contraloría General de la República y que son de cumplimiento para las entidades pertenecientes al Sistema Nacional de Control Peruano.

Referenciado en: Página 48, correspondiente al numeral 1.1 del Capítulo 1 del presente trabajo de tesis.

A continuación, se detalla la normativa identificada para el presente trabajo de tesis:

Reglamento de los Órganos de Control Institucional

	Resolución	Fecha de Promulgación	Fecha de Publicación	Denominación
1	RC N° 459-2008-CG	28/10/2008	30/10/2008	Contralor General autoriza aprobar Reglamento de los Órganos de Control Institucional
2	RC N° 99-2010-CG	21/04/2010	23/04/2010	Modifican el Reglamento de los Órganos de Control Institucional

Normas de Control Interno

	Resolución	Fecha de Promulgación	Fecha de Publicación	Denominación
1	RC N° 320-2006-CG	30/10/2006	03/11/2006	Aprueban las Normas de Control Interno

Normas de Auditoría Gubernamental

	Resolución	Fecha de Promulgación	Fecha de Publicación	Denominación
1	RC N° 162-95-CG	22/09/1995	26/09/1995	Aprueban las Normas de Auditoría Gubernamental
2	RC N° 141-99-CG	25/11/1999	29/11/1999	Modifican Normas y Manual de Auditoria Gubernamental
3	RC N° 259-2000-CG	07/12/2000	13/12/2000	Modifican Normas de Auditoría Gubernamental
4	RC N° 12-2002-CG	21/01/2002	22/01/2002	Sustituyen texto de la Norma de Auditoría Gubernamental 4.50 - Informe Especial
5	RC N° 89-2002-CG	09/05/2002	11/05/2002	Suspende obligación de remitir Informes Especiales al Comité de Calidad de la Contraloría General, dispuesta por la NAGU 4.50.

Manual de Auditoría Gubernamental

	Resolución	Fecha de Promulgación	Fecha de Publicación	Denominación
1	RC N° 152-98-CG	18/12/1998	19/12/1998	Aprueba: [1] Manual de Auditoría Gubernamental, [2]Guía de Planeamiento de Auditoría Gubernamental, [3]Guía de Elaboración del Informe de Auditoría Gubernamental, [4]Guía de Papeles de Trabajo
2	RC N° 141-99-CG	25/11/1999	29/11/1999	Modifican Normas y Manual de Auditoria Gubernamental

Implementación de recomendaciones

	Resolución	Fecha de Promulgación	Fecha de Publicación	Denominación
1	RC N° 279-2000-CG	29/12/2000	30/12/2000	Aprueban Directiva N° 14-2000-CG/B150 - Directiva para la Verificación y Seguimiento de implementación de recomendaciones derivadas de Informes de Acciones de Control

Anexo N° 3
Detalle de los 133 controles de la NTP ISO-IEC/17799-2007

Objetivo: Identificar los controles establecidos en la NTP ISO-IEC/17799-2007 relacionados a las buenas prácticas para la implementación de controles en los sistemas de gestión de seguridad de la información.

Referenciado en: Página 49, correspondiente al numeral 1.2 del Capítulo 1 del presente trabajo de tesis.

A continuación, se detallan los 133 controles de la NTP ISO-IEC/17799-2007, distribuidos en 39 Categorías que a su vez conforman 11 Cláusulas:

CLAUSULAS y CATEGORÍAS												
5. Política de Seguridad			**6. Aspectos organizativos para la seguridad**			**7. Clasificación y control de activos**			**8. Seguridad en recursos humanos**		
5.1	Política de seguridad de la información		6.1	Organización interna		7.1	Responsabilidad sobre los activos		8.1	Seguridad antes del empleo	
	5.1.1	Documento de la Política de seguridad de la información		6.1.1	Comité de gestión de seguridad de la información		7.1.1	Inventario de activos		8.1.1	Inclusión de la seguridad en las responsabilidades y funciones laborales
	5.1.2	Revisión y evaluación		6.1.2	Coordinación de la seguridad de la información		7.1.2	Propiedad de los activos		8.1.2	Selección y política de personal
				6.1.3	Asignación de responsabilidades sobre seguridad de la información		7.1.3	Uso adecuado de los activos		8.1.3	Acuerdos de confidencialidad
				6.1.4	Proceso de autorización de recursos para el tratamiento de la información						
				6.1.5	Acuerdos de confidencialidad						
				6.1.6	Contacto con autoridades						
				6.1.7	Contacto con grupos de interés especial						
				6.1.8	Revisión independiente de la seguridad de la información						
			6.2	Seguridad en los accesos de terceras partes		7.2	Clasificación de la información		8.2	Durante el empleo	
				6.2.1	Identificación de riesgos por el acceso de terceros		7.2.1	Guías de clasificación		8.2.1	Responsabilidades de la gerencia
				6.2.2	Requisitos de seguridad cuando sea trata con clientes		7.2.2	Marcado y tratamiento de la información		8.2.2	Conocimiento, educación y entrenamiento de la seguridad de información
				6.2.3	Requisitos de seguridad en contratos de outsourcing					8.2.3	Proceso disciplinario
									8.3	Finalización o cambio del empleo	
										8.3.1	Responsabilidades de finalización
										8.3.2	Retorno de activos

								8.3.3	Retiro de los derechos de acceso

CLAUSULAS y CATEGORÍAS											
9. Seguridad física y del entorno			**10. Gestión de comunicaciones y operaciones**			**11. Control de accesos**			**12. Adquisición, desarrollo y mantenimiento de sistemas**		
9.1	Áreas seguras		10.1	Procedimientos y responsabilidades de operación		11.1	Requisitos de negocio para el control de accesos		12.1	Requisitos de seguridad de los sistemas	
	9.1.1	Perímetro de seguridad física		10.1.1	Documentación de procedimientos operativos		11.1.1	Política de control de accesos			
	9.1.2	Controles físicos de entradas		10.1.2	Gestión de Cambios						
	9.1.3	Seguridad de oficinas, despachos y recursos		10.1.3	Segregación de tareas						
	9.1.4	Protección contra amenazas externas y ambientales		10.1.4	Separación de los recursos para desarrollo y para producción						
	9.1.5	El trabajo en las áreas seguras									
	9.1.6	Acceso publico, áreas de carga y descarga									
9.2	Seguridad de los equipos		10.2	Gestión de servicios externos		11.2	Gestión de acceso de usuarios		12.2	Seguridad de las aplicaciones del sistema	
				10.2.1	Servicio de entrega		11.2.1	Registro de usuarios		12.2.1	Validación de los datos de entrada
				10.2.2	Monitoreo y revisión de los servicios externos		11.2.2	Gestión de privilegios		12.2.2	Control del proceso interno
				10.2.3	Gestionando cambios para los servicios externos		11.2.3	Gestión de contraseñas de usuario		12.2.3	Integridad de mensajes
							11.2.4	Revisión de los derechos de acceso de los usuarios		12.2.4	Validación de los datos de salida
			10.3	Planificación y aceptación del sistema		11.3	Responsabilidades de los usuarios		12.3	Controles criptográficos	
				10.3.1	Planificación de la capacidad		11.3.1	Uso de contraseñas		12.3.1	Política de uso de los controles criptográficos
				10.3.2	Aceptación del sistema		11.3.2	Equipo informático de usuario desatendido		12.3.2	Gestión de claves
							11.3.3	Política de pantalla y escritorio limpio			
			10.4	Protección contra software malicioso		11.4	Control de acceso a la red		12.4	Seguridad de los archivos del sistema	
				10.4.1	Medidas y controles contra software malicioso		11.4.1	Política de uso de los servicios de la red		12.4.1	Control del software en producción
				10.4.2	Medidas y controles contra código móvil		11.4.2	Autentificación de usuario para conexiones externas		12.4.2	Protección de los datos de prueba del sistema
							11.4.3	Identificación de equipos en las redes		12.4.3	Control de acceso a los códigos de programas fuente
							11.4.4	Diagnostico remoto y configuración de protección de puertos			

						11.4.5	Segregación en las redes			
						11.4.6	Control de conexión a las redes			
						11.4.7	Control de enrutamiento en la red			
		10.5	Gestión de respaldo y recuperación		11.5	Control de acceso al sistema operativo		12.5	Seguridad en los procesos de desarrollo y soporte	
			10.5.1	Recuperación de la información		11.5.1	Procedimientos de conexión de terminales		12.5.1	Procedimientos de control de cambios
						11.5.2	Identificación y autenticación del usuario		12.5.2	Revisión técnica de los cambios en el sistema operativo
						11.5.3	Sistema de gestión de contraseñas		12.5.3	Restricciones en los cambios a los paquetes de software
						11.5.4	Utilización de las facilidades del sistema		12.5.4	Fuga de Información
						11.5.5	Desconexión automática de sesiones		12.5.5	Desarrollo externo del software
						11.5.6	Limitación del tiempo de conexión			
		10.6	Gestión de seguridad en redes		11.6	Control de acceso a las aplicaciones y la información		12.6	Gestión de la vulnerabilidad técnica	
			10.6.1	Controles de red		11.6.1	Restricción de acceso a la información		12.6.1	Control de las vulnerabilidades técnicas
			10.6.2	Seguridad en los servicios de redes		11.6.2	Aislamiento de sistemas sensibles			
		10.7	Utilización de los medios de información		11.7	Informática móvil y teletrabajo				
			10.7.1	Gestión de medios removibles		11.7.1	Informática móvil y comunicaciones			
			10.7.2	Eliminación de medios		11.7.2	Teletrabajo			
			10.7.3	Procedimientos de manipulación de la información						
			10.7.4	Seguridad de la documentación de sistemas						
		10.8	Intercambio de información							
			10.8.1	Políticas y procedimientos para el intercambio de información y software						
			10.8.2	Acuerdos de Intercambio						
			10.8.3	Medios físicos en tránsito						
			10.8.4	Seguridad en la mensajería electrónica						
			10.8.5	Sistemas de Información de Negocios						
		10.9	Servicios de correo electrónico							
			10.9.1	Comercio Electrónico						
			10.9.2	Transacciones en línea						

			10.9.3	Información publica disponible				
		10.10	Monitoreo					
			10.10.1	Registro de la auditoria				
			10.10.2	Monitoreando el uso del sistema				
			10.10.3	Protección de la información de registro				
			10.10.4	Registro de administradores y operadores				
			10.10.5	Registro de la avería				
			10.10.6	Sincronización del reloj				

CLAUSULAS y CATEGORÍAS								
13. Gestión de incidentes en la seguridad de información			**14. Gestión de continuidad del negocio**			**15. Cumplimiento**		
13.1	Reportando eventos y debilidades de la seguridad de información		14.1	Aspectos de la gestión de continuidad del negocio		15.1	Cumplimiento con los requisitos legales	
	13.1.1	Reportando los eventos en la seguridad de información		14.1.1	Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio		15.1.1	Identificación de la legislación aplicable
	13.1.2	Reportando debilidades en la seguridad de información		14.1.2	Continuidad del negocio y evaluación de riesgos		15.1.2	Derechos de propiedad intelectual (DPI)
				14.1.3	Redacción e implantación de planes de continuidad que incluyen la seguridad de información		15.1.3	Salvaguarda de los registros de la organización
				14.1.4	Marco de planificación para la continuidad del negocio		15.1.4	Protección de los datos y de la privacidad de la información personal
				14.1.5	Prueba, mantenimiento y reevaluación de los planes de continuidad		15.1.5	Prevención en el mal uso de los recursos de tratamiento de la información
							15.1.6	Regulación de los controles criptográficos
13.2	Gestión de las mejoras e incidentes en la seguridad de información					15.2	Revisiones de la política de seguridad y de la conformidad técnica	
	13.2.1	Responsabilidades y procedimientos					15.2.1	Conformidad con la política de seguridad y los estándares
	13.2.2	Aprendiendo de los incidentes en la seguridad de información					15.2.2	Comprobación de la conformidad técnica
	13.2.3	Recolección de evidencia						
						15.3	Consideraciones sobre la auditoria de sistemas	
							15.3.1	Controles de auditoria de sistemas
							15.3.2	Protección de las herramientas de auditoria de sistemas
Total: 39 Categorías								

Anexo N° 4
Marco Legal emitido por la ONGEI – PCM

Objetivo: Identificar la normatividad emitida por la Presidencia del Consejo de Ministros República y que es de cumplimiento para las entidades del sector público peruano.

Referenciado en: Página 51, correspondiente al numeral 1.2 del Capítulo 1 del presente trabajo de tesis.

A continuación, se detalla la normativa identificada para el presente trabajo de tesis:

Norma	Fecha de Promulgación	Fecha de Publicación	Denominación
RM N° 013-2003-PCM	12/02/2003	13/02/2003	Dictan medidas para garantizar la legalidad de la adquisición de programas de software en entidades y dependencias del Sector Público
RM N° 073-2004-PCM	16/03/2004	17/03/2004	Aprueban documento "Guía Técnica sobre evaluación de software para la administración pública"
RM N° 139-2004-PCM	27/05/2004	28/05/2004	Aprueban Guía para la Administración eficiente del software legal en la Administración Pública
RM N° 179-2004-PCM	14/06/2004	15/06/2004	Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2004 Tecnología de la Información. "Procesos del Ciclo de Vida del Software, 1ª Edición" en entidades del Sistema Nacional de Informática.
DS N° 037-2005-PCM	09/05/2005	11/05/2005	Modifican el D.S. N° 013-2003-PCM, fijando plazo para que las entidades cumplan con inventariar los software que utilizan
DS N° 024-2006-PCM	22/05/2006	24/05/2006	Aprueban Reglamento de la Ley N° 28612 - Ley que norma el uso, adquisición y adecuación del software en la Administración Pública
DS N° 002-2007-PCM	10/01/2007	11/01/2007	Modifican el D.S. N° 013-2003-PCM y establecen disposiciones referidas a licenciamiento de software en entidades públicas
RM N° 246-2007-PCM	22/08/2007	25/08/2007	Aprueban uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI Tecnología 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 [Adopción de la norma ISO/IEC 27002:2005]
DS N° 52-2008-PCM	18/07/2008	19/07/2008	Reglamento de la Ley 27269 - Ley de Firmas y Certificados Digitales
DS N° 053-2008-PCM	08/08/2008	09/08/2008	Modifica el artículo 4° del Decreto Supremo N° 013-2003-PCM para el cumplimiento de la Administración Pública de las normas vigentes en materia de Derechos de Autor en el Marco de la Reforma del Estado y la implementación del Acuerdo de Promoción Comercial Perú - Estados Unidos
DS N° 077-2008-PCM	26/11/2008	27/11/2008	Modifican el Artículo 4º del Decreto Supremo Nº 013-2003-PCM para el cumplimiento en la Administración Pública de las normas vigentes en materia de derechos de autor en el marco de la reforma del Estado y la implementación del Acuerdo de Promoción Comercial Perú - Estados Unidos
DS Nº 76-2010-PCM	23/07/2010	24/07/2010	Decreto Supremo que modifica el Decreto Supremo Nº 013-2003-PCM estableciendo disposiciones referidas a las adquisiciones de computadoras personales que convoquen las entidades públicas
RM N° 129-2012-PCM	23/05/2012	25/05/2012	Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de la seguridad de la información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática. [Adopción de la norma ISO/IEC 27001:2005]

Anexo N° 5
Detalle de los 210 Objetivos de Control Específicos – COBIT 4.1

Objetivo: Identificar los controles establecidos en COBIT 4.1 relacionados a las buenas prácticas para un adecuado Gobierno de las Tecnologías de Información.

Referenciado en: Página 57, correspondiente al numeral 1.4.2 del Capítulo 1 del presente trabajo de tesis.

A continuación, se detallan los 210 controles de COBIT 4.1, distribuidos en 34 procesos (objetivos de control de alto nivel) agrupados en 4 dominios:

DOMINIOS Y OBJETIVOS DE CONTROL												
PLANIFICAR Y ORGANIZAR (Planificar)			**ADQUIRIR E IMPLANTAR (Construir)**			**ENTREGAR Y DAR SOPORTE (Ejecutar)**			**MONITOREAR Y EVALUAR (Monitorear)**		
PO1	Definir el plan estratégico de TI		AI1	Identificar soluciones automatizadas.		DS1	Definir y administrar niveles de servicio.		ME1	Monitorear y evaluar el desempeño de TI.	
	PO1.1	Administración del valor de TI		AI1.1	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.		DS1.1	Marco de administración de niveles de servicio		ME1.1	Enfoque del Monitoreo
	PO1.2	Alineación de TI con el negocio		AI1.2	Reporte de análisis de riesgos		DS1.2	Definiciones de los servicios		ME1.2	Definición y recolección de datos de monitoreo
	PO1.3	Evaluación del desempeño y la capacidad actual		AI1.3	Estudio de factibilidad y formulación de cursos alternativos de acción		DS1.3	Acuerdos de niveles de servicio (ANS)		ME1.3	Método de monitoreo
	PO1.4	Plan estratégico de TI		AI1.4	Requerimientos, decisión de factibilidad y aprobación.		DS1.4	Acuerdos de niveles de operación		ME1.4	Evaluación del desempeño
	PO1.5	Planes tácticos de TI					DS1.5	Monitoreo y reporte del cumplimento de los niveles de servicio		ME1.5	Reportes al Consejo Directivos y a ejecutivos
	PO1.6	Administración del portafolio de TI					DS1.6	Revisión de los acuerdos de niveles de servicio y de los contratos		ME1.6	Acciones correctivas
PO2	Definir la arquitectura de la información		AI2	Adquirir y mantener el software aplicativo.		DS2	Administrar servicios de terceros.		ME2	Monitorear y evaluar el control interno	
	PO2.1	Modelo de arquitectura de información empresarial		AI2.1	Diseño de alto nivel		DS2.1	Identificación de todas las relaciones con proveedores		ME2.1	Monitoreo del marco de trabajo del control interno
	PO2.2	Diccionario de datos empresarial y reglas de sintaxis de datos		AI2.2	Diseño detallado		DS2.2	Administración de relaciones con proveedores		ME2.2	Revisiones de Supervisión
	PO2.3	Esquema de clasificación de datos		AI2.3	Control y auditabilidad de las aplicaciones		DS2.3	Administración de riesgos de proveedores		ME2.3	Excepciones de control
	PO2.4	Administración de integridad		AI2.4	Seguridad y disponibilidad de las aplicaciones.		DS2.4	Monitoreo del desempeño de proveedores		ME2.4	Autoevaluación de control

				AI2.5	Configuración e implementación de software aplicativo adquirido					ME2.5	Aseguramiento del control interno
				AI2.6	Actualizaciones importantes en sistemas existentes					ME2.6	Control interno para terceros
				AI2.7	Desarrollo de software aplicativo					ME2.7	Acciones correctivas
				AI2.8	Aseguramiento de la calidad del software						
				AI2.9	Administración de los requisitos de las aplicaciones						
				AI2.10	Mantenimiento del software aplicativo						
PO3	Determinar la dirección tecnológica		AI3	Adquirir y mantener la infraestructura tecnológica		DS3	Administrar desempeño y capacidad.		ME3	Garantizar cumplimiento regulatorio.	
	PO3.1	Planeación de la orientación tecnológica		AI3.1	Plan de adquisición de infraestructura tecnológica		DS3.1	Planeamiento del desempeño y la capacidad		ME3.1	Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales
	PO3.2	Plan de infraestructura tecnológica		AI3.2	Protección y disponibilidad de la infraestructura		DS3.2	Capacidad y desempeño actual		ME3.2	Optimizar la Respuesta a Requerimientos Externos
	PO3.3	Monitoreo de tendencias y regulaciones futuras		AI3.3	Mantenimiento de la Infraestructura		DS3.3	Capacidad y desempeño futuro		ME3.3	Evaluación del Cumplimiento con Requerimientos Externos
	PO3.4	Estándares tecnológicos		AI3.4	Ambiente de prueba de factibilidad		DS3.4	Disponibilidad de recursos de TI		ME3.4	Aseguramiento Positivo del Cumplimiento
	PO3.5	Consejo de arquitectura de TI					DS3.5	Monitoreo y reporte		ME3.5	Reportes Integrados
PO4	Definir procesos, organización y relaciones de TI		AI4	Facilitar la operación y el uso.		DS4	Garantizar la continuidad del servicio.		ME4	Proporcionar gobierno de TI.	
	PO4.1	Marco de trabajo de procesos de TI		AI4.1	Planificación de soluciones operacionales		DS4.1	Marco de trabajo de continuidad de TI		ME4.1	Establecer un marco de trabajo de gobierno para TI
	PO4.2	Comité estratégico de TI		AI4.2	Transferencia de conocimiento a la Gerencia del negocio		DS4.2	Planes de continuidad de TI		ME4.2	Alineamiento estratégico
	PO4.3	Comité directivo de TI		AI4.3	Transferencia de conocimiento a los usuarios finales		DS4.3	Recursos críticos de TI		ME4.3	Entrega de valor
	PO4.4	Ubicación organizacional de la función de TI		AI4.4	Transferencia de conocimiento al personal de operaciones y soporte		DS4.4	Mantenimiento del plan de continuidad de TI		ME4.4	Administración de recursos
	PO4.5	Estructura organizacional de TI					DS4.5	Pruebas del plan de continuidad de TI		ME4.5	Administración de riesgos
	PO4.6	Establecer roles y responsabilidades					DS4.6	Entrenamiento en el plan de continuidad de TI		ME4.6	Medición del desempeño
	PO4.7	Responsabilidades para el aseguramiento de la calidad de TI (QA)					DS4.7	Distribución del plan de continuidad de TI		ME4.7	Aseguramiento independiente

	PO4.8	Responsabilidad sobre el riesgo, la seguridad y el cumplimiento					DS4.8	Recuperación y reanudación de los servicios de TI			
	PO4.9	Propiedad de los datos y sistemas					DS4.9	Almacenamiento externo y respaldos			
	PO4.10	Supervisión					DS4.10	Revisión post-reanudación			
	PO4.11	Segregación de funciones									
	PO4.12	Personal de TI									
	PO4.13	Personal clave de TI									
	PO4.14	Políticas y procedimientos para el personal contratado									
	PO4.15	Relaciones									
PO5	Administrar la inversión en TI		AI5	Adquirir recursos de TI.		DS5	Garantizar la seguridad de los sistemas.				
	PO5.1	Marco de trabajo para la administración financiera		AI5.1	Control de adquisiciones		DS5.1	Administración de la seguridad de TI			
	PO5.2	Priorización dentro del presupuesto de TI		AI5.2	Administración de contratos de proveedores		DS5.2	Plan de seguridad de TI			
	PO5.3	Proceso presupuestal		AI5.3	Selección de proveedores		DS5.3	Administración de identidad			
	PO5.4	Administración de costos de TI		AI5.4	Adquisición de recursos de TI		DS5.4	Administración de cuentas del usuario			
	PO5.5	Administración de beneficios					DS5.5	Pruebas, vigilancia y monitoreo de la seguridad			
							DS5.6	Definición de incidente de seguridad			
							DS5.7	Protección de la tecnología de seguridad			
							DS5.8	Administración de llaves criptográficas			
							DS5.9	Prevención, detección y corrección de software malicioso			
							DS5.10	Seguridad de la red			
							DS5.11	Intercambio de datos sensitivos			
PO6	Comunicar las aspiraciones y la dirección de la Gerencia		AI6	Administrar cambios.		DS6	Identificar y asignar costos.				
	PO6.1	Política y entorno de control de TI		AI6.1	Estándares y procedimientos para cambios		DS6.1	Definición de servicios			
	PO6.2	Riesgo corporativo y marco de referencia del control interno de TI		AI6.2	Evaluación de impacto, priorización y autorización		DS6.2	Contabilización de TI			
	PO6.3	Administración de políticas para TI		AI6.3	Cambios de emergencia		DS6.3	Modelamiento de costos y cargos			

	PO6.4	Implantación de políticas, estándares y procedimientos de TI		AI6.4	Seguimiento y reporte de estado de los cambios		DS6.4	Mantenimiento del modelo de costos		
	PO6.5	Comunicación de los objetivos y la dirección de TI		AI6.5	Cierre y documentación del cambio					
PO7	Administrar recursos humanos de TI		AI7	Instalar y acreditar soluciones y cambios.		DS7	Educar y entrenar a los usuarios.			
	PO7.1	Reclutamiento y retención del personal		AI7.1	Entrenamiento		DS7.1	Identificación de necesidades de educación y formación		
	PO7.2	Competencias del personal		AI7.2	Plan de pruebas		DS7.2	Brindar educación y entrenamiento		
	PO7.3	Asignación de roles		AI7.3	Plan de implementación		DS7.3	Evaluación del entrenamiento recibido		
	PO7.4	Entrenamiento del personal de TI		AI7.4	Ambiente de prueba					
	PO7.5	Dependencia de individuos		AI7.5	Conversión de datos y sistemas					
	PO7.6	Verificación de antecedentes del personal		AI7.6	Pruebas de cambios					
	PO7.7	Evaluación del desempeño del empleado		AI7.7	Pruebas de aceptación final					
	PO7.8	Cambios y ceses en los puestos de trabajo		AI7.8	Promoción a producción					
				AI7.9	Revisión posterior a la implementación					
PO8	Administrar calidad					DS8	Administrar la mesa de servicio y los incidentes.			
	PO8.1	Sistema de administración de calidad					DS8.1	Mesa de Servicios		
	PO8.2	Estándares y prácticas de calidad					DS8.2	Registro de consultas de clientes		
	PO8.3	Estándares para desarrollos y adquisiciones					DS8.3	Escalamiento de incidentes		
	PO8.4	Enfoque en el cliente de TI					DS8.4	Cierre de incidentes		
	PO8.5	Mejora continua					DS8.5	Reportes y análisis de tendencias		
	PO8.6	Medición, monitoreo y revisión de la calidad								
PO9	Evaluar y administrar riesgos de TI					DS9	Administrar la configuración.			
	PO9.1	Marco de trabajo de administración de riesgos					DS9.1	Repositorio y línea base de configuración		
	PO9.2	Establecimiento del contexto del riesgo					DS9.2	Identificación y mantenimiento de elementos de configuración		
	PO9.3	Identificación de eventos					DS9.3	Revisión de integridad de la configuración		

	PO9.4	Evaluación de riesgos de TI							
	PO9.5	Respuesta a los riesgos							
	PO9.6	Mantenimiento y monitoreo de un plan de acción de riesgos							
P10	Administrar proyectos				DS10	Administrar los problemas.			
	PO10.1	Marco de trabajo para la administración de programas				DS10.1	Identificación y clasificación de problemas		
	PO10.2	Marco de trabajo para la administración de proyectos				DS10.2	Seguimiento y resolución de problemas		
	PO10.3	Enfoque de administración de proyectos				DS10.3	Cierre de problemas		
	PO10.4	Compromiso de los interesados				DS10.4	Integración de la administración de configuración, incidentes y problemas		
	PO10.5	Declaración de alcance del proyecto							
	PO10.6	Inicio de las fases del proyecto							
	PO10.7	Plan integrado del proyecto							
	PO10.8	Recursos del proyecto							
	PO10.9	Administración de riesgos del proyecto							
	PO10.10	Plan de calidad del proyecto							
	PO10.11	Control de cambios del proyecto							
	PO10.12	Planeamiento del proyecto y métodos de aseguramiento							
	PO10.13	Medición del desempeño, reporte y monitoreo del proyecto							
	PO10.14	Cierre del proyecto							
					DS11	Administrar los datos.			
						DS11.1	Requerimientos del negocio para la administración de datos		
						DS11.2	Acuerdos para el almacenamiento y la conservación		
						DS11.3	Sistema de administración de librerías de medios		
						DS11.4	Eliminación		

					DS11.5	Respaldo y restauración		
					DS11.6	Requisitos de seguridad para la administración de datos		
				DS12	Administrar el ambiente físico.			
					DS12.1	Selección y diseño del centro de datos		
					DS12.2	Medidas de seguridad física		
					DS12.3	Acceso Físico		
					DS12.4	Protección contra factores ambientales		
					DS12.5	Administración de instalaciones físicas		
				DS13	Administrar las operaciones.			
					DS13.1	Procedimientos e instrucciones de operación		
					DS13.2	Programación de tareas		
					DS13.3	Monitoreo de la infraestructura de TI		
					DS13.4	Documentos sensitivos y dispositivos de salida		
					DS13.5	Mantenimiento preventivo del hardware		
Subtotal: 74		**Subtotal:** 40		**Subtotal:** 71			**Subtotal:** 25	
Total: 210 Objetivos de Control Específicos								