UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

“AUDITORÍA INTERNA GUBERNAMENTAL INFORMÁTICA EVALUACIÓN DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN, DE UNA ENTIDAD AUTÓNOMA Y DESCENTRALIZADA”

TESIS

PRESENTADA A LA HONORABLE JUNTA DIRECTIVA DE LA FACULTAD DE CIENCIAS ECONÓMICAS

POR

CHRISTIAN DAVID SUMALE CHOCOJ

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

Guatemala, noviembre de 2016

MIEMBROS DE LA JUNTA DIRECTIVA
FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. Luis Antonio Suárez Roldán
Secretario	Lic. Carlos Roberto Cabrera Morales
Vocal Segundo	Lic. Calos Alberto Hernández Gálvez
Vocal Tercero	Lic. Juan Antonio Gómez Monterroso
Vocal Cuarto	P.C. Marlon Geovani Aquino Abdalla
Vocal Quinto	P.C. Carlos Roberto Turcios Pérez

PROFESIONALES QUE REALIZARON
LOS EXÁMENES DE ÁREAS PRÁCTICAS BÁSICAS

Área Matemática-Estadística	Lic. Jorge Orlando Recinos Sandoval
Área Contabilidad	Lic. Ronaldo Antonio López Ortiz
Área Auditoría	Lic. Manuel Fernando Morales García

PROFESIONALES QUE REALIZARON EL
EXAMEN PRIVADO DE TESIS

Presidente	Lic. Hugo Vidal Requena Beltetón
Secretario	Lic. Herson Ulises Fuentes Velásquez
Examinador	Lic. Manuel Alberto Selva Rodas

Guatemala, 24 de mayo de 2016

Licenciado
Luis Antonio Suarez Roldan
Decano de la Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala

Respetable Señor Decano:

De conformidad con la designación contenida en el DICTAMEN-AUDITORÍA 325-2015 del 18 de noviembre de 2015 del Secretario de la Junta Directiva de la Facultad de Ciencias Económicas con visto bueno de su Persona, para asesorar al Perito Contador **Christian David Sumale Chocoj**, carné **200920270-1** en su trabajo de tesis denominado "**AUDITORÍA INTERNA GUBERNAMENTAL INFORMÁTICA EVALUACIÓN DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN, DE UNA ENTIDAD AUTÓNOMA Y DESCENTRALIZADA**", le informo que, de conformidad con la revisión efectuada, el trabajo indicado llena los requisitos que el reglamento establece.

El trabajo referido constituye un valioso aporte para los profesionales de las ciencias económicas, empresas, instituciones y personas interesadas en el estudio de la auditoría de tecnologías de información; además, en vista de la trascendencia del tema, la investigación realizada reviste particular relevancia. En tal virtud, en opinión del suscrito, el trabajo presenta una investigación cuya actualidad y calidad, reúne los requisitos académicos necesarios que el caso amerita.

Con base en lo anteriormente expuesto, recomiendo que el trabajo realizado sea aprobado para su presentación, por el señor Christian David Sumale Chocoj, en el examen privado de tesis, previo a conferírsele el título de Contador Público y Auditor en el grado académico de Licenciado.

Atentamente,

Licenciado Erik Roberto Flores López
Contador Público y Auditor
No. de Colegiado 303

c.c. archivo

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS
EDIFICIO "S-8"
Ciudad Universitaria zona 12
GUATEMALA, CENTROAMERICA

DECANATO DE LA FACULTAD DE CIENCIAS ECONÓMICAS, GUATEMALA ONCE DE OCTUBRE DE DOS MIL DIECISÉIS.

Con base en el Punto QUINTO, inciso 5.8, subinciso 5.8.1 del Acta 18-2016 de la sesión celebrada por la Junta Directiva de la Facultad el 04 de octubre de 2016, se conoció el Acta AUDITORÍA 157-2016 de aprobación del Examen Privado de Tesis, de fecha 11 de agosto de 2016 y el trabajo de Tesis denominado: "AUDITORÍA INTERNA GUBERNAMENTAL INFORMÁTICA, EVALUACIÓN DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN, DE UNA ENTIDAD AUTÓNOMA Y DESCENTRALIZADA ", que para su graduación profesional presentó el estudiante **CHRISTIAN DAVID SUMALE CHOCOJ,** autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

LIC. LUIS ANTONIO SUÁREZ ROLDÁN
DECANO

m.ch

DEDICATORIA

A DIOS:	Por permitirme llegar a este momento tan importante, por darme la sabiduría, fortaleza y perseverancia.
A MI MADRE:	Marina Chocoj Méndez de Sumale Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor.
A MI PADRE:	Walter Paul Sumale Valenzuela Por haberme apoyado en todo momento y por sus consejos.
A MIS ABUELOS:	En especial a Maria Juana Méndez García y Guillermo Chocoj Por quererme y apoyarme siempre.
A MI ESPOSA:	Joseline Betzabe Ortiz Gonzalez Por cada momento compartido en mi carrera profesional, pero sobre todo por creer en mí y exhortarme a perseverar.
A MI HIJO:	Diego Adrián Sumale Ortiz Que este triunfo sirva de ejemplo para superación en su vida.
A MI HERMANA:	Nahomi Marissa Sumale Chocoj Por sus muestras de amor y cariño.
A MIS TIOS:	En especial a Maria Antonieta Méndez García e Italo Vinicio Ardón Suruy Por su apoyado en todo momento.
A MIS AMIGOS:	En especial a Erick René Pérez Guerra y Christopher William Clark Alvarado Triunfo que comparto con ustedes como agradecimiento a su amistad.
A LOS LICENCIADOS:	Esmelin Casasola Fajardo y Erwin Obduilio Ericastilla Mejía Por el apoyado en la realización de este triunfo.
A LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA:	Por haber permitido mi formación como profesional.
A USTED:	Que comparte conmigo el triunfo que he alcanzado.

ÍNDICE

CAPÍTULO IV
AUDITORÍA INTERNA GUBERNAMENTAL INFORMÁTICA, EVALUACIÓN DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN, DE UNA ENTIDAD AUTÓNOMA Y DESCENTRALIZADA
(CASO PRÁCTICO)

ÍNDICE DE FIGURAS

INTRODUCCIÓN

La constante y veloz evolución de la tecnología de la información y las comunicaciones en el mundo de hoy, significa grandes avances en todos los ámbitos del quehacer humano, desde las ciencias astronómicas hasta la educación y la salud, en los rincones más remotos de la Tierra; sin embargo, acompañando a este gran avance tecnológico, cada día aparecen riesgos y retos que es necesario gestionar adecuadamente para que, lo que parece ser una solución, no se convierta en un problema.

Una de las herramientas que constituye un factor de éxito para la prevención de pérdidas no esperadas en todo tipo de organizaciones es la gestión de riesgos, a través de la cual se puede identificar las amenazas y/o vulnerabilidades actuales para darles el tratamiento adecuado y minimizar el impacto de una eventual pérdida. Como parte de las mejores prácticas que hoy existen en el mundo, la gestión de riesgos se enmarca dentro de un concepto aún mayor, que constituye el gobierno corporativo, los riesgos y el cumplimiento (GRC), cuyas directrices y objetivos se complementan entre sí, y ponen en relieve la importancia del gobierno de la tecnología de información (TI).

Estudios en diversas industrias demuestran que existen varias ventajas en la implementación de un buen gobierno de tecnologías de la información, tales como la mejora en el retorno de las inversiones, mejor imagen y reputación, mayor satisfacción de los clientes o usuarios en la obtención de productos y servicios, mayor creación de valor para las partes interesadas de las organizaciones, entre otros.

En este contexto, el conocimiento y aplicación de herramientas que permitan diagnosticar el riesgo existente en la gestión tecnológica y conocer las áreas en las que deben enfocarse los esfuerzos, es fundamental para la optimización del gobierno corporativo y de tecnologías de la información de las organizaciones. En el caso de las instituciones públicas de Guatemala, muy poco se hace por mejorar

su gobierno de tecnologías de la información, debido a factores como la falta de información del mismo o, simplemente, porque las mismas deben priorizar en otros asuntos que a criterio de sus autoridades son más importantes que la adecuada implementación de un gobierno de tecnologías de la información que les ayude a mejorar sus servicios, siendo estos oportunos y adecuados a cada uno de sus usuarios.

En el presente trabajo, se expondrá en el capítulo I, que es una entidad autónoma y descentralizada, porque se originan su tipo de organización, características principales, la clasificación que se da en el territorio guatemalteco sus objetivos como se rigen su presupuesto y como el gobierno garantiza su adecuado funcionamiento con su ente fiscalizador que dentro de las funciones del mismo se encuentra mejorar cada día, elementos como trasparencia en el manejo de sus fondos y calidad de los servicios que presta.

En el capítulo II, se expone la auditoría interna gubernamental informática, sus antecedentes los tipos de auditoria gubernamental que estipula la Contraloría General de Cuentas, el origen de las auditorias informáticas gubernamentales, los tipos de auditorías informáticas que plantea el sistema de auditoría gubernamental para unidades de auditoría interna, que es una auditoría de gobierno de tecnologías de la información, sus generalidades los marcos que rigen este tipo de auditoría.

En el capítulo III, se expone los marcos, estándares y buenas practicas que indican el cómo debe realizarse la auditoría de gobierno de tecnologías de la información del cual no se puede dejar de lado las normas gubernamentales que rigen el accionar de las unidades de auditoría interna de las instituciones de gobierno, las normas para el ejercicio profesional de la auditoría interna, marcos de referencia como COBIT, las normas ISO, específicamente la 38500 y la familia de las 27000, que son un marco de evaluación del ambiente de control.

En el capítulo IV, se presenta el caso práctico que amalgama la teoría descrita en los anteriores capítulos y que expone las necesidades de las instituciones públicas

por su falta de gestión en el fortalecimiento de su marco regulatorio que tiene que ver con sus tecnologías de la información, que se va conociendo con la ejecución de la auditoria de gobierno de tecnologías de la información.

Por último, se presentan las conclusiones y recomendaciones a las cuales se arribó como consecuencia de la investigación realizada y la bibliografía utilizada.

CAPÍTULO I
ENTIDADES AUTONOMAS Y DESCENTRALIZADAS

1.1 Antecedentes

De acuerdo con lo prescrito por el artículo 134 de la Constitución, en Guatemala existen entes que gozan de autonomía por mandato constitucional, situación en la que se encuentran algunos organismos, instituciones y entidades estatales que, debido a su inherente naturaleza, se les ha asignado competencias y atribuciones especiales, tales como los organismos Legislativo y Judicial, el Tribunal Supremo Electoral, cuyas determinaciones en materia de contratación o adquisición de bienes y servicios no pueden estar supeditadas a trámites o aprobaciones por parte del Organismo Ejecutivo, por cuanto ello implicaría una injerencia ilegítima e inaceptable en su independencia funcional y una grave vulneración a su estatus constitucional. En tanto a otras les corresponde una autonomía restringida con un concreto fin de descentralización administrativa, que les ha sido o les puede ser conferida por medio de una ley ordinaria. De aquí que sea jurídicamente factible distinguir, dentro de la organización del Estado guatemalteco, entes cuya autonomía, por ser de rango constitucional, sólo podría ser suprimida mediante una modificación a la Constitución, y entes descentralizados o semiautónomos que tiene su origen en una ley ordinaria, que pueden ser suprimidos por medio de otra ley de igual categoría votada por una mayoría calificada de diputados al Congreso de la República, supresión referida sólo a éstas últimas, como claramente lo dispone el párrafo final del citado artículo 134. Esta circunstancia explica que unos y otros pueden merecer, en determinadas situaciones jurídicas tratamientos diferentes.

1.1.1 Autonomía

El diccionario de la lengua española define la autonomía como: "Potestad que dentro de un Estado tienen municipios, provincias, regiones u otras entidades, para regirse mediante normas y órganos de gobierno propios." (12)

También se define como: el derecho que tiene una institución de elegir sus autoridades, darse sus reglamentos, dictar sus planes, preparar su presupuesto y orientar sus funciones o actividades con independencia del Estado.

La autonomía es la transferencia de competencia o funciones administrativas del Estado a personas jurídicas públicas o privadas, sobre las cuales el Estado ejerce control administrativo.

Dicha autonomía consiste en dirigir, organizar y desarrollar las actividades por cuenta propia.

"La autonomía, fuera de los casos especiales contemplados en la Constitución Política de la República de Guatemala, se considera únicamente, cuando se estime indispensable para la mayor eficiencia de la entidad y el mejor cumplimiento de sus fines". (1:30)

1.2 Creación u origen

Las entidades descentralizadas y autónomas del Estado, son creadas por la Constitución Política de la República de Guatemala, éstas deben propiciar cambios que favorezcan al desarrollo social, como un proceso dinámico que se produce por la interacción de los diferentes agentes sociales en el devenir histórico, por medio del cual se transforman constantemente las estructuras sociales, en la búsqueda de mejores condiciones materiales y espirituales de los integrantes de la sociedad. Se cuenta para esto, con las instituciones descentralizadas y autónomas, como las entidades del Estado para cumplir con los objetivos fijados y para satisfacer las necesidades de toda comunidad.

Su importancia consiste en que se tiende a la satisfacción de necesidades, mediante la prestación de un servicio y su objetivo radica en el mejoramiento de la práctica administrativa, para servir mejor a los intereses públicos.

Los mecanismos por medio de los cuales se constituyen las diferentes entidades del Estado, en autónomas o semiautónomas, centralizadas o descentralizadas, están otorgadas por varias leyes; entre las más importantes se pueden mencionar,

la Constitución Política de la República de Guatemala, la cual indica que: las entidades descentralizadas pueden ser autónomas y semiautónomas, y que para crear las entidades descentralizadas y autónomas, será necesario el voto favorable de las dos terceras partes del Congreso de la República, así también, les asigna atribuciones específicas de acuerdo a su naturaleza.

En su artículo 134, preceptúa que: "el municipio y las entidades autónomas y descentralizadas, actúan por delegación del Estado, y les establece como obligaciones mínimas las siguientes:

- Coordinar su política, con la política general del Estado y, en su caso, con la especial del ramo a que correspondan;
- Mantener estrecha coordinación con el órgano de planificación del Estado;
- Remitir para su información al Organismo Ejecutivo y al Congreso de la República, sus presupuestos detallados ordinarios y extraordinarios, con expresión de programas, proyectos, actividades ingresos y egresos. Se exceptúa a la Universidad de San Carlos de Guatemala. Tal remisión será con fines de aprobación, cuando así lo disponga la ley;
- Remitir a los mismos organismos, las memorias de sus labores y los informes específicos que les sean requeridos, queda a salvo el carácter confidencial de las operaciones de los particulares en los bancos e instituciones financieras en general;
- Dar facilidades necesarias para que el órgano encargado del control fiscal, pueda desempeñar amplia y eficazmente sus funciones; y,
- En toda actividad de carácter internacional, sujetarse a la política que trace el Organismo Ejecutivo." (1:30)

"De considerarse inoperante el funcionamiento de una entidad autónoma o descentralizada, será suprimida mediante el voto favorable de las dos terceras partes del Congreso de la República." (1:30)

1.2.1 Organización

Las entidades autónomas se organizan bajo un sistema staff, donde la autoridad inicia de forma descendente, de acuerdo a su naturaleza, alcance, funciones y/o atribuciones.

Las entidades autónomas, son instituciones que tienen libertad de gobernarse y regirse por sus propias leyes; además, gozan de personalidad jurídica y patrimonio propio; sin embargo, debe considerarse que aunque algunas de ellas constitucionalmente son autónomas, dentro de sus leyes orgánicas, se indica que su autonomía es funcional, razón por la cual deben cumplir con la presentación de sus Proyectos de Presupuesto al Organismo Ejecutivo, para fines de aprobación, sus leyes son necesarias para su funcionamiento. Aunque reciben un aporte por parte del Estado, dichas entidades no tienen ningún vínculo con relación a éste.

Se puede concluir que las entidades autónomas: son personas jurídicas a las cuales el Estado, constitucional o legalmente, delegó su actuación, en competencia y funciones administrativas, ejerciendo únicamente un control administrativo sobre ellas.

Según el artículo 16, del Decreto Ley Número 106 "Código Civil", indica que: "la personalidad jurídica, consiste en una forma de entidad civil distinta de sus miembros individualmente considerados; puede ejercitar todos los derechos y contraer obligaciones que sean necesarias para realizar sus fines y será representada por la persona u órgano que designe la ley, las reglas de su institución, sus estatutos o reglamentos". (7:4)

1.3 Características

Cada entidad autónoma debe reunir ciertas características, las que difieren según sus funciones y/o atribuciones; para distinguir y concordar sus características, se hace referencia a la clasificación respectiva descrita a continuación.

1.4 Clasificación

Las entidades autónomas en Guatemala se pueden clasificar en:

- Entidades autónomas territoriales,
- Establecimientos públicos,
- Empresas industriales o comerciales del Estado y
- Sociedades de economía mixta o estatales.

1.5 Entidades autónomas territoriales

Son las que también pueden transferir competencia administrativa a personas jurídicas públicas o privadas distintas, entre éstas se pueden mencionar a las Municipalidades; cuya característica es transferir competencia administrativa a personas jurídicas públicas o privadas distintas a las del Estado, en una localidad determinada.

1.5.1 Objetivos

A pesar que cada entidad autónoma tiene diferentes objetivos específicos, se puede deducir que el objetivo, en forma general, radica en el mejoramiento de la práctica administrativa, para servir mejor a los intereses públicos.

1.5.2 Presupuesto

Los presupuestos de las entidades autónomas, al igual que las dependencias del Estado, deben ser elaborados según los principios presupuestales de anualidad, unidad, equilibrio, programación y publicidad, en tal virtud deben:

- Corresponder a un ejercicio fiscal anual;
- Contener agrupados y clasificados, en un solo documento, todos los recursos y gastos estimados para dicho ejercicio;
- Estructurarse en forma tal que exista correspondencia entre los recursos y gastos, a efecto que éstos se conformen mediante una programación basada fundamentalmente en los planes de desarrollo; y,
- Hacerse del conocimiento público.

Las entidades autónomas enviarán sus presupuestos anualmente al Ejecutivo y al Congreso de la República de Guatemala, para su conocimiento e integración al presupuesto General, cuando sea con fines de aprobación.

La Ley Orgánica del Presupuesto, Decreto Número 101-97, establece en su artículo 1, Objeto. "La presente Ley tiene por finalidad normar, los sistemas presupuestarios, de contabilidad integrada gubernamental, de tesorería, y de crédito público". (8:1)

1.6 Ente fiscalizador

La Ley Orgánica del Presupuesto, en su artículo 17, Decreto Número 101-97, preceptúa que: "la fiscalización de los presupuestos del sector público sin excepción, será ejercida por la Contraloría General de Cuentas o por la Superintendencia de Bancos de Guatemala, según sea el caso". (8:2)

El artículo 1, del Decreto Número 31-2002 del Congreso de la Republica, indica que "la Contraloría General de Cuentas es una institución técnica y descentralizada. De conformidad con esta ley, goza de independencia funcional, técnica y administrativa, y con competencia en todo el territorio nacional, con capacidad para establecer delegaciones en cualquier lugar de la República". (6:2)

El Articulo 2, establece que: "corresponde a la Contraloría General de Cuentas la función fiscalizadora en forma externa de los activos y pasivos, derechos, ingresos y egresos y, en general, todo interés hacendario de los Organismos del Estado, entidades autónomas y descentralizadas, las municipalidades y sus empresas, y demás instituciones que conforman el sector público no financiero; de toda persona, entidad o institución que reciba fondos del Estado o haga colectas públicas; de empresas no financieras en cuyo capital participe el Estado, bajo cualquier denominación, así como las empresas en que éstas tengan participación". (6:2)

Según el artículo 4 del mismo cuerpo legal, señala que: "esta Entidad tiene asignadas las funciones y/o atribuciones siguientes:

- Ser el órgano rector de control gubernamental. Las disposiciones, políticas y procedimientos que dicte en el ámbito de su competencia, son de observancia y cumplimiento obligatorio para los organismos, instituciones, entidades y demás personas a que se refiere el artículo 2 de la presente ley;
- Efectuar el examen de operaciones y transacciones financieras-administrativas a través de la práctica de auditorías con enfoque integral a los organismos, instituciones, entidades y demás personas a que se refiere el artículo 2 de esta ley, emitiendo el informe sobre lo examinado de acuerdo con las normas de auditoría gubernamental interna y externa, vigentes;
- Normar el control interno institucional y la gestión de las unidades de auditoría interna, proponiendo las medidas que contribuyan a mejorar la eficiencia y eficacia de las mismas, incluyendo las características que deben reunir los integrantes de dichas unidades;
- Evaluar los resultados de la gestión de los organismos, instituciones, entidades y personas a que se refiere el artículo 2 de la presente ley, bajo los criterios de probidad, eficacia, eficiencia, transparencia, economía y equidad;
- Auditar, emitir dictamen y rendir informe de los estados financieros, ejecución y liquidación del Presupuesto General de Ingresos y Egresos del Estado, y los de las entidades autónomas y descentralizadas, enviando los informes correspondientes al Congreso de la República, dentro del plazo constitucional;
- Promover de oficio y ser parte actora de los Juicios de Cuentas en contra de los funcionarios y empleados públicos que no hubieren desvanecido los reparos o cargos formulados por la Contraloría General de Cuentas;
- Requerir a la autoridad nominadora, la suspensión en forma Inmediata del funcionario o empleado público encargado de la custodia, manejo y administración de los valores públicos, cuando se hubieren detectado

hechos presuntamente constitutivos de delito, vinculados con sus atribuciones y, además, denunciarlos ante las autoridades competentes;

- Nombrar interventores en los asuntos de su competencia, de carácter temporal, en los organismos, instituciones o entidades sujetas a control, cuando se compruebe que se está comprometiendo su estabilidad económica-financiera;
- Autorizar los formularios, sean estos impresos o en medios informáticos, destinados a la recepción de fondos y egresos de bienes muebles y suministros, a excepción de aquellos referentes a los aspectos administrativos de las entidades a que se refiere el artículo 2 de esta ley, así como controlar y fiscalizar su manejo;
- Examinar la contabilidad de los contratistas de obras públicas y de cualquier persona individual o jurídica que, por delegación del Estado, reciba, invierta o administre fondos públicos, así como en aquellas en que el Estado delegue la administración, ejecución o supervisión de obras o servicios públicos, en lo relacionado con fondos del Estado;
- Autorizar y verificar la correcta utilización de las hojas movibles, libros principales y auxiliares que se operen en forma manual, electrónica o por otros medios legalmente autorizados de las entidades sujetas a fiscalización;
- Cuando las circunstancias lo demanden y de manera exclusiva, calificar y contratar Contadores Públicos y Auditores Independientes, que sean colegiados activos en forma individual o como firmas de auditoría, para realizar auditorías en los organismos, entidades y personas a que se refiere el artículo 2 de la presente ley, quedando sujetas éstas a la supervisión de la Contraloría General de Cuentas;
- Promover la eficiencia profesional de los auditores gubernamentales, a través de un plan de capacitación y actualización continua;
- Promover mecanismos de lucha contra la corrupción;

- Verificar la veracidad de la información contenida en las declaraciones de probidad presentadas por los funcionarios y empleados públicos, de conformidad con la ley de la materia y la presente Ley;
- De acuerdo con las características de las entidades sujetas a examen, la Contraloría General de Cuentas podrá contratar especialistas de otras disciplinas profesionales para que participen en las auditorías, debiendo estos emitir un Dictamen Técnico de acuerdo con su especialidad;
- Ejercer control de las emisiones de las especies postales, fiscales, de bonos, cupones y otros documentos o títulos de la deuda pública emitidos por el Estado o del municipio, billetes de lotería nacional o cualesquiera otros documentos o valores que determine la ley;
- Controlar la incineración o destrucción de cédulas, bonos, cupones y cualesquiera otros documentos o títulos de crédito del Estado o del municipio y demás instituciones sujetas a su fiscalización;
- Emitir opinión o dictámenes sobre asuntos de su competencia que le sean requeridos por los Organismos del Estado o entidades sujetas a fiscalización". (6:3)

CAPÍTULO II
AUDITORÍA INTERNA GUBERNAMENTAL INFORMÁTICA

2.1 Antecedentes

Debido a los cambios experimentados en las entidades públicas de Guatemala, con la incorporación de tecnologías de punta, que modifican las metodologías de trabajo en los diferentes niveles administrativos y operativos de las entidades, el Ministerio de Finanzas Públicas implementó el Sistema Integrado de Administración Financiera y Sistema de Auditoría Gubernamental (SIAF- SAG), así como el Sistema de Contabilidad Integrada (SICOIN), con el fin de simplificar e integrar la ejecución presupuestaria y financiera de las diferentes actividades y alcanzar los resultados con eficiencia y eficacia de las instituciones del Estado. Para que estos procesos funcionen y puedan ejecutarse, deben diseñarse las políticas metodológicas, normas, técnicas, procedimientos y demás disposiciones para poder ejercer el control interno y externo de las dependencias del sector gubernamental.

La Contraloría General de Cuentas, conjuntamente con la Unidad de Auditoría Interna de cada entidad, debe mantener el control de las operaciones por medio de un proceso sistemático que evalúe y revise a través de pruebas y evaluaciones constantes, basadas en Normas de Auditoría Gubernamental Interna y Externa, determinando el resultado operativo respecto a la integridad del control.

La ejecución de la fase III del Proyecto SIAF-SAG, incluye el fortalecimiento de la administración financiera, así como del control interno que conforme a la legislación vigente y la normativa técnica emitida, le corresponde ejercer a la propia administración.

El Decreto Número 31-2002 del Congreso de la República, Ley Orgánica de la Contraloría General de Cuentas, establece en el artículo 6, que "esta institución debe normar lo relativo a las actividades técnicas que ejercerán las unidades de auditoría interna de los organismos, instituciones y entidades del Estado". (6:5)

En este contexto, la Auditoría Interna, en cumplimiento de la ley, debe organizarse y definir sus funciones, de tal manera que le permita evaluar todo el ámbito operacional, cuando aplique, para cumplir con las responsabilidades establecidas en las Normas de Auditoría Gubernamental Interna y Externa emitidas por la Contraloría General de Cuentas.

Las Unidades de Auditoría Interna (UDAI´s), deben actuar como asesores gerenciales en todos los campos de la institución a la que pertenecen, basado en los exámenes que realiza para determinar la eficiencia, efectividad y economía con que las instituciones realizan la planificación, la ejecución, control e información de sus actividades, producto de lo cual, proporciona recomendaciones para la actualización y mejoramiento de la organización institucional y los sistemas en funcionamiento.

Constituye asimismo, el mejor elemento que garantiza la funcionalidad y permanencia de un ambiente y estructura de control interno sólidos, en todos los niveles, para ayudar a la protección y uso adecuado de los recursos.

Por esta razón, las UDAI´s, requieren del apoyo irrestricto de la administración y específicamente de la máxima autoridad, de tal manera que se garantice:

- Una organización adecuada a las necesidades institucionales,
- Un enfoque y cobertura conforme a la normativa técnica y legal,
- La contratación del personal técnico necesario,
- La provisión de herramientas de trabajo suficientes y modernas,
- Una capacitación permanente de los auditores, y
- El apoyo a la independencia de los auditores internos.

2.1.1 Tipos de auditoría

La Contraloría General de Cuentas tipifica las clases o tipos de auditoría como a continuación se detalla:

- Auditoría financiera
- Auditoría de gestión

- Auditoría de informática
- Auditoría de obra pública
- Examen especial
- Auditoría integral
- Auditorías especializadas

"Éstas las pueden realizar las unidades de auditoría Interna y cualquier otro auditor independiente". (6:12)

2.1.1.1 Auditoría financiera

"Evalúa los estados financieros y la liquidación del presupuesto, con el fin de dar una opinión profesional e independiente sobre la razonabilidad del contenido de los mismos, incluyendo la revisión de toda la evidencia que sustenta su veracidad." (6:12)

2.1.1.2 Auditoría de gestión

"Evalúa el proceso administrativo y operacional, con el fin de determinar si la organización, funciones, sistemas integrados y procedimientos diseñados para el control de las operaciones, se ajustan a las necesidades institucionales, profesionales y técnicas, para promover la eficiencia, efectividad y economía en la conducción de las operaciones y en el logro de los resultados, así como el impacto de los mismos en la comunidad." (6:13)

2.1.1.3 Auditoría informática

"Evalúa los sistemas de información, para medir la conveniencia y capacidad de los recursos tecnológicos asignados, para la optimización de los procesos de información y toma de decisiones de los entes públicos y la sostenibilidad de los mismos." (6:13)

2.1.1.4 Auditoría de obra pública

"Evalúa los proyectos de inversión y fiscaliza las obras públicas finalizadas dentro de los programas establecidos, para medir si los logros alcanzados se ajustan a

las especificaciones técnicas y presupuestarias, en el marco de las políticas gubernamentales." (6:13)

2.1.1.5 Examen especial

"Se refiere a la evaluación de aspectos limitados como un rubro de los estados financieros, así como cualquier tema operacional y financiero, y otros que tengan que ver con irregularidades y fraudes sobre los recursos del Estado, para establecer las causas de las desviaciones y los montos de la lesión patrimonial, de ser el caso, para promover acciones correctivas, legales, la recuperación y sanción correspondiente." (6:13)

2.1.1.6 Auditoría integral

"Consiste en un enfoque de trabajo que promueve la interacción de los responsables administrativos y técnicos de las operaciones y los auditores gubernamentales, en la búsqueda de soluciones globales para los males que aquejan individualmente a los entes públicos, y a estos dentro del sector al que pertenecen." (6:13)

2.1.1.7 Auditorías especializadas

"Se refieren a metodologías de trabajo que tienen que ver con: la seguridad social, la educación, el servicio de energía eléctrica, la ecología, el medio ambiente y otros trabajos especializados que ayudan a la optimización de los recursos asignados a los entes públicos responsables."(6:13)

Estas definiciones enmarcan la postura del ente fiscalizador gubernamental pero otros definiciones la identifican como *la revisión práctica que se realiza sobre los recursos informáticos con que cuenta una entidad con el fin de emitir un informe o dictamen sobre la situación en que se desarrollan y se utilizan esos recursos.*

2.2 Origen de la auditoría interna gubernamental

Los inicios de la auditoría se remontan a la revisión y el diagnóstico que se practicaban a los registros de las operaciones contables de las empresas; luego al

análisis, verificación y evaluación de sus aspectos financieros; posteriormente, se amplió al examen de algunos rubros de la administración, siguiendo el análisis de aquellos aspectos que intervenían en todas las actividades y, por último, su alcance se incrementó conforme se avanzó en la llamada revisión integral. Actualmente llega a las revisiones especializadas de algunas áreas y actividades específicas que se desempeñan en las instituciones.

En Guatemala la auditoría en general inicia en el año 1937, cuando se crea la Facultad de Ciencias Económicas de la Universidad de San Carlos de Guatemala por medio del decreto 1972, difundido por el presidente de aquella época el general Jorge Ubico, pero fue en el año 1943 cuando egresó el primer profesional de las ciencias económicas.

Con la revolución de 1944, se abre paso a políticas de régimen revolucionario que promueven el desarrollo económico, social, político y cultural del país; políticas que causan un profundo impacto en las funciones de la administración pública y la actividad productiva, que determinan una importante demanda de profesionales de la ciencias económicas en instituciones y empresas de nueva creación, como:

- Ministerio de Economía y de Trabajo
- Banco de Guatemala
- Instituto Guatemalteco de Seguridad Social
- Instituto de Fomento de la Producción
- Departamento de Fomento Cooperativo, etc.

Los cambios institucionales y la política económica de los gobiernos revolucionarios, dan auge al estudio de las ciencias económicas; estudiantes y profesionales juegan un papel importante en la orientación política y económica del país.

La auditoría surgió como producto de una necesidad social generado por el desarrollo económico, con el propósito de otorgar máxima transparencia de la administración en la información económica y financiera. Y nace en cumplimiento de las disposiciones establecidas en la Ley Orgánica de la Contraloría General de

Cuentas, Decreto Número 31-2002, "como entidad rectora de la fiscalización de las operaciones de las entidades del Estado". (6:5)

El control del sector público gubernamental: comprende un conjunto de actividades y acciones técnicas y legales, ejercidas por la Contraloría General de Cuentas, y las unidades de auditoría interna, para evaluar todo el ámbito operacional, funcional y legal de los entes públicos por medio de prácticas modernas de auditoría, accionado por profesionales que no intervienen en las actividades u operaciones controladas, con las normas de auditoría del sector público no financiero, técnicas y procedimientos que permitan un enfoque objetivo y profesional, y cuyos resultados se sinteticen en recomendaciones para mejorar la administración pública.

2.3 Origen de las auditorias informáticas gubernamentales

A finales del siglo XX, los sistemas informáticos se constituyeron en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial.

La auditoría nace como un órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico-financiero, y los casos inmediatos, se encuentran en las peritaciones judiciales y las contrataciones de contables expertos por parte de bancos oficiales.

La Informática, en la actualidad, está enfocada en la gestión integral de la empresa o entidad y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se denominó el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa o entidad, existe la Auditoría Informática.

El término de Auditoría se empleó en algunos casos incorrectamente ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas.

Si se consulta el Boletín de normas de auditoría del Instituto Mexicano de contadores nos dice: La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo son de carácter indudable.

Las normas para el ejercicio profesional de la auditoria interna (NIEPAI), emitidas por el Instituto de Auditores Interno Global, la define como: "una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno". (17)

De todo esto se deduce que la auditoría es un examen crítico, pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Los principales objetivos que constituyen a la auditoría Informática son el control de la función informática; el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normativa general de la empresa o entidad en este ámbito; y, la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

En los últimos años, el sector público de Guatemala, experimenta cambios trascendentales, principalmente en lo que respecta a la incorporación de tecnologías de punta, traducidas en el uso de herramientas computacionales que modifican las metodologías de trabajo en los diferentes niveles operativos de las entidades, con el objetivo de hacer que los diferentes procesos se ejecuten en forma ágil, oportuna y confiable.

El sistema de administración financiera gubernamental y sus diferentes procesos, regulados por el Decreto Número 101-97 del Congreso de la República, Ley Orgánica del Presupuesto, "son objeto de rediseño utilizando la herramienta informática denominada: Sistema de Contabilidad Integrada (SICOIN), con el fin de simplificar la ejecución de las diferentes actividades, para alcanzar resultados con eficiencia, eficacia y economía; sin embargo, estos procesos de rediseño no pueden ejecutarse independientemente del fortalecimiento del control gubernamental". (8:15)

Según el artículo 232, de la Constitución Política de la República de Guatemala, "la Contraloría General de Cuentas tiene la potestad de evaluar y pronunciarse sobre el manejo de fondos y bienes públicos" (1,44); por su parte, el artículo 4, literal a), de la Ley orgánica de la Contraloría General de Cuentas, Decreto Número 31-2002 del Congreso de la República, le asigna la atribución de "ser el órgano rector del control gubernamental; y, en ese contexto, es la única entidad responsable de implementar un Sistema de Auditoría del Sector Gubernamental". (6:3)

La vigencia de los estatutos propuestos por la Contraloría General de Cuentas, se explican por sí solos, por cuanto el compromiso es de contribuir al mejoramiento de la administración financiera del Estado, por medio de un trabajo profesional e independiente.

La Contraloría General de Cuentas, basada en su responsabilidad constitucional y la necesidad permanente de asegurar la calidad de los servicios que ofrece al sector público y a la ciudadanía, revisa, actualiza y emite las Normas de Auditoría para el sector Gubernamental, cuyo texto reúne experiencias del ejercicio profesional en los nuevos ambientes tecnológicos del sector público, técnicas de la profesión contable a nivel nacional y de autores destacados en el ámbito internacional, así como de los organismos especializados que regulan la profesión de la auditoría.

Los constantes cambios en el ambiente gubernamental, exigieron una acción fiscalizadora calificada y consistente con los avances tecnológicos y la aplicación de diferentes tendencias y filosofías que promueven cambios constantes en los entes públicos; en tal sentido, la Contraloría General de Cuentas, puso en vigencia las Normas de Auditoría para el sector Gubernamental, quedando como una responsabilidad permanente el contribuir, a través de sus autoridades y auditores gubernamentales, internos y externos, para que las Normas de Auditoría Gubernamental sean aplicadas y actualizadas oportunamente, como un medio de retroalimentación para que los sistemas sean evaluados en todas las entidades públicas y funcionen en forma eficiente, para que la gestión institucional sea más productiva, de tal manera que se manifieste el valor agregado de la profesión.

Esto contribuiría a elevar el nivel de calidad de la función de la Contraloría General de Cuentas, que como entidad superior de control, debe implantar y darle sostenibilidad a metodologías de trabajo que sean acordes con los avances tecnológicos, para estar a la altura de los más calificados despachos de firmas privadas de auditoría, para que los trabajos de Auditoría del sector Gubernamental, se encuentren dentro de un contexto moderno de la profesión y bajo estándares exigidos por el ambiente cambiante de la administración pública, así como congruente con los sistemas integrados de administración y finanzas, y con otros procedimientos que utilizan las instituciones en su diario ejercicio operacional, procurando alcanzar sus objetivos en forma eficiente, efectiva y económica.

Es por eso que la Contraloría General de Cuentas, por medio del acuerdo A-059-2011, crea la Unidades de Auditoría Gubernamental en Sistemas Informáticos, las que dentro de sus funciones principales contempla la verificación del control interno establecido en el área de sistemas, estudios de seguridad física y lógica (análisis de los riesgos a que está expuesta la información y los equipos), la elaboración de documentación y recomendaciones e informes resultados de las auditorías practicadas fortaleciendo la gestión, seguimiento, fiscalización,

evaluación y cumplimiento de los sistemas informáticos para alcanzar transparencia en la gestión pública.

Los principales objetivos de la unidad de auditoría gubernamental en sistemas informáticos, planteados por la Contraloría General de Cuentas, son:

- Salvaguardar los activos
- Razonabilidad e integridad de los datos
- Efectividad de sistemas
- Eficiencia de sistemas
- Seguridad y confidencialidad

2.4 Tipos de auditoría informática gubernamental

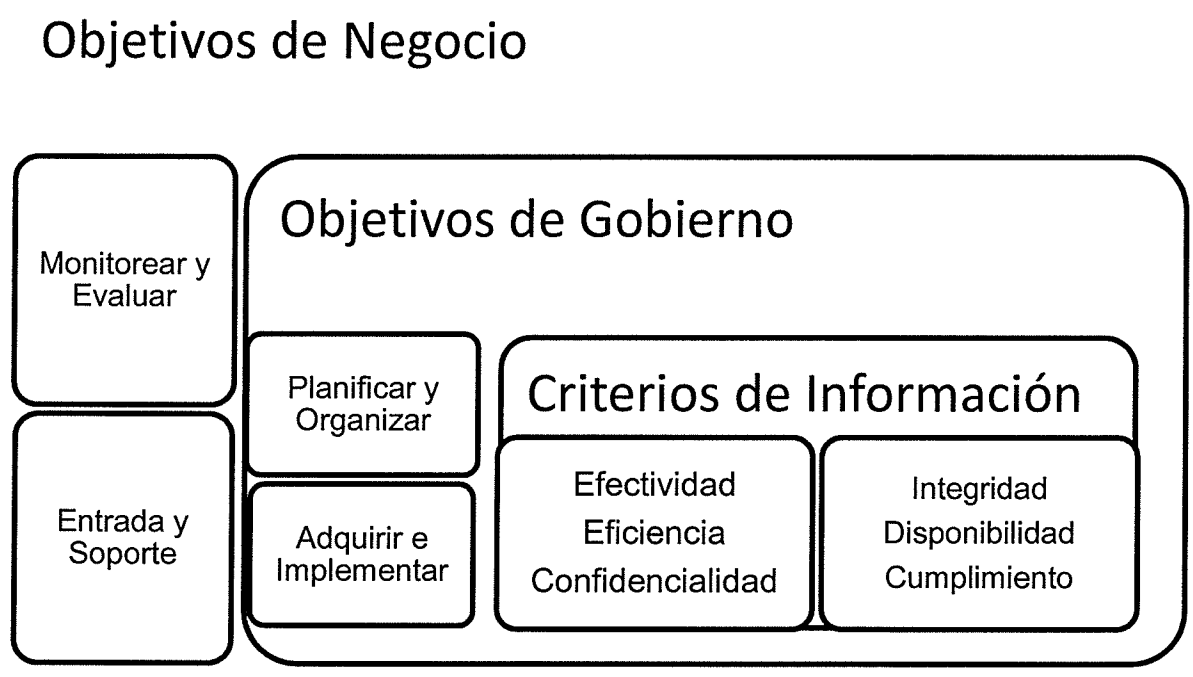
La Contraloría General de Cuentas, dentro del Sistema de Auditoría Gubernamental, indica que las unidades de auditoría interna y auditores independientes, realizarán distintos tipos de auditoría, dependiendo de las circunstancias, necesidades y prioridades establecidas en el Plan Anual de Auditoría (PAA), de tal forma que en ninguno de sus estatutos indica que tipos de auditoría deberá realizarse, únicamente establece las posibles áreas de evaluación para cada uno de los distintos tipos de auditoría que establecen las normas gubernamentales.

Por su parte el sistema gubernamental, SAG UDAI, establece las áreas a auditar para practicar auditoría informática, dichas áreas se apegan a la estructura del marco de referencia COBIT 4.1, (Control Objectives for Information and related Technology por sus siglas en ingles), que se abordaran más adelante, el que se divide en dominios que son agrupaciones de procesos que corresponden a una responsabilidad personal, procesos que son una serie de actividades unidas con delimitación o cortes de control y objetivos de control o actividades requeridas para lograr un resultado medible, para administrar y gobernar la información y tecnología relacionada en toda la empresa.

En la actualidad COBIT 5, define 37 procesos que contienen prácticas de gobierno o prácticas de administración, según sea proceso de gobierno, el cual puede ser Evaluación y Monitoreo Directo (EDM por sus siglas en inglés); o proceso de Administración como Alinear, Planificar y Organizar (APO por sus siglas en inglés); Construir, Adquirir e Implementar (BAI por sus siglas en inglés); Entrega, Servicio y Soporte (DSS por sus siglas en inglés); y, Supervisar, Evaluar y Valorar (MEA por sus siglas en inglés), si bien el marco de referencia que se utiliza es COBIT 4.1 ya que este es la base en la cual se fundamenta el sistema gubernamental SAG UDAI, también se empleara COBIT 5 para establecer las "áreas de evaluación de la Auditoria Informática Gubernamental y definir objetivos de control generales, para cada uno de los procesos de las tecnologías de la información". (8:41) Sobre este marco de referencia se ampliará en el capítulo III.

Figura 1

Modelo de Referencia de Procesos de COBIT 4.1



Fuente: COBIT 4.1, ISACA.

La clasificación de las áreas propuestas por la Contraloría General de Cuentas, para auditoría informática, se dividen en cuatro áreas de evaluación enfocada o referenciadas al marco de aplicación COBIT 4.1 descrito con anterioridad, ya que las mismas comparten similitudes con los dominios propuestos por este marco de referencia, de aspectos que a consideración del ente fiscalizador gubernamental son las posibles áreas a evaluar dentro de una auditoría informática, las que a continuación se describen:

a.	**Planificación y organización**
1	Plan estratégico para tecnologías de información
2	Arquitectura de la información
3	Dirección tecnológica
4	Proceso, organización y relación de TI
5	Administración de la inversión en TI
6	Comunicación de las aspiraciones de la gerencia
7	Administración de los recursos humanos en TI
8	Administración de la calidad
9	Evaluación y administración de riesgos de TI
b.	**Adquisición e implementación**
1	Identificación de soluciones automatizadas
2	Adquisición y mantenimiento de software
3	Adquisición y mantenimiento de infraestructura tecnología
4	Facilitación de operaciones y uso
5	Adquisición de recursos de TI
6	Administración de cambios
7	Instalación y acreditamiento de soluciones y cambios
c.	**Entrega y soporte técnico**
1	Definición y administración de niveles de servicio
2	Administración de servicios a terceros
3	Administración del desempeño y la capacidad
4	Garantía de continuidad del servicio
5	Garantía en la seguridad de los sistemas
6	Identificación y asignación de costos
7	Educación y entrenamiento a usuarios
8	Administración de mesa de servicios e incidentes
9	Administración de la configuración
10	Administración de problemas
11	Administración de datos
12	Administración de ambientes físicos

13	Administración de operaciones
d.	**Monitoreo y Evaluación**
1	Monitoreo y evaluación al desempeño de TI
2	Monitoreo y evaluación al control interno
3	Garantía del cumplimiento regulatorio
4	Proporcionar gobierno de TI

2.5 Auditoría de gobierno de tecnologías de la información

La información es un recurso clave para todas las empresas, y en todo el ciclo de vida de la información corporativa, existe una enorme dependencia de la tecnología.

El gobierno de tecnologías de la información provee las estructuras que unen los procesos de tecnologías de la información, los recursos de tecnologías de la información y la información con las estrategias y los objetivos de la empresa; además, el gobierno de tecnologías de la información integra e institucionaliza buenas (o mejores) prácticas de planificación y organización; adquisición e implementación; entrega de servicios y soporte; y, monitoriza el rendimiento de TI para asegurar que la información de la empresa y las tecnologías relacionadas soportan sus objetivos del negocio.

El gobierno de tecnologías de la información, conduce a la empresa a tomar total ventaja de su información, logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva.

Una estructura de relaciones y procesos, para dirigir y controlar la empresa, con el fin de alcanzar los objetivos de la empresa y añadir valor mientras se equilibran los riesgos y el retorno sobre tecnologías de la información y sus procesos.

El núcleo de tecnologías de la información consta de dos responsabilidades principales, la entrega de valor al negocio y mitigar los riesgos relacionados con tecnologías de la información. La gerencia de la organización necesita ampliar sus responsabilidades de gobierno a tecnologías de información y proveer estructuras y procesos, que aseguren que las tecnologías de la información son capaces de soportar los objetivos y estrategias de la organización.

Cada implementación de gobierno de tecnologías de la información se lleva a cabo en diferentes condiciones y circunstancias (entorno de Gobierno de TI) determinados por factores tales como:

- Ética y cultura de la organización y de la industria.
- Leyes, regulaciones y guías vigentes, tanto internas como externas.
- Misión, visión y valores de la organización.
- La organización de la organización de sus roles y responsabilidades.
- Intenciones estratégicas y tácticas de la organización.

2.5.1 Generalidades de la auditoría de tecnologías de la información

La terminología utilizada en el ámbito informático suele ser muy propios de está, es por ello que se darán a conocer conceptos generales, mismos que permitirán comprender mejor la presente investigación.

- **Sistema de información (SI):** Un sistema de información "está formado por todos los componentes que colaboran para procesar los datos y producir información." (12:11) En una organización, un sistema de información está formado por los datos, el hardware, y software, las telecomunicaciones, las personas y los procedimientos. Por ello "un sistema de información se ha vuelto un sinónimo de un sistema de información basado en computadoras." (12:13)
- **Tecnología de la información (TI):** La tecnología de la información (TI), se refiere a la interacción entre el hardware, software y comunicaciones.
- **Hardware:** "Se entiende como el conjunto de aparatos que conforman una computadora". (12:111)

Software: Es "una serie de instrucciones para que una computadora ejecute uno o varios procesos, como mostrar textos, manipular números, copiar o eliminar documentos." (12:147)

2.5.2 Marcos regulatorios de las tecnologías de la información

La necesidad de cumplir con requerimientos regulatorios para controles de las tecnologías de la información distintos países como: Estados Unidos de América, España, Alemania entre otros, encaminaron y dieron la pauta para garantizar la privacidad de la información como ejemplos se mencionan: Sarbanes-Oxley, Basilea III, ley orgánica de protección de datos de carácter personal, ley de servicios de la sociedad de la información y comercio electrónico y otros, y en sectores específicos como el financiero, salud, telecomunicaciones e internet, seguros, farmacéutico y otros.

Iniciativas de gobierno de tecnologías de la información, que incluyen la adopción de marcos de referencia de control y de mejores prácticas para ayudar a monitorear y mejorar las actividades críticas de las TI, aumentar el valor del negocio y reducir sus riesgos como en los que se detallan a continuación:

- Riesgos cada vez más complejos de las TI
- La conectividad entre las redes y su seguridad

La necesidad de optimizar y minimizar los costes siguiendo un enfoque estandarizado en lugar de enfoques individualizados

La madurez y concienciación creciente y la aceptación de marcos de trabajo respetados tales como: COBIT, ITIL, ISO/IEC 38500, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 2700; así como, catálogos de protección de niveles mínimos de tecnologías de la información, entre otros.

2.5.3 Origen y desarrollo de la auditoría de tecnologías de información

"La primera entidades que incursiono en el referido tema es ISACA, conformada por personas que reconocieron la necesidad de contar con una fuente centralizada de información y guías en el creciente campo de la auditoría a los controles de los sistemas computacionales.

ISACA comenzó en 1967, por un pequeño grupo de personas objetivos similares, auditar controles en los sistemas computacionales que eran cada vez más críticos para las operaciones de sus respectivas organizaciones, por lo que se discute la necesidad de tener una fuente centralizada de información y guías en dicho campo. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor en el campo de gobierno y control de TI. Conocida previamente como la Information Systems Audit and Control Association (Asociación de Auditoría y Control en Sistemas de Información), ISACA ahora es solo un acrónimo, que refleja la amplia gama de profesionales en gobierno de TI a los que sirve." (15)

2.5.4 El rol de la auditoría en el gobierno de tecnologías de la información

La auditoría tiene un rol significativo en una implementación exitosa del gobierno de tecnologías de información dentro de la organización. Provee importantes recomendaciones de prácticas a la alta dirección, para ayudar a mejorar la calidad y la efectividad de las iniciativas del gobierno de tecnologías de información implementadas, y asegura el cumplimiento de las iniciativas para dicho gobierno

El Auditor de Sistemas de Información necesita evaluar como mínimo los siguientes aspectos:

- La alineación de la función de las tecnologías de la información con la misión, la visión, los valores, los objetivos y las estrategias de la organización.
- El logro por parte de la función de las tecnologías de la información de los objetivos de desempeño establecidos por el negocio.
- Los requerimientos legales, ambientales de calidad de la información fiduciarios, de seguridad y privacidad.
- El ambiente de control de la organización.
- Inversión versus gastos en tecnologías de la información.

CAPÍTULO III

NORMAS PARA PRACTICAR AUDITORÍA INFORMÁTICA GUBERNAMENTAL

3.1 La constitución política de la república de Guatemala

La Constitución Política de la República de Guatemala en su artículo 232 indica que: la Ley Orgánica de la Contraloría de Cuentas, otorgan a ésta última competencia para fiscalizar ingresos, egresos y en todo aquello de interés hacendario de los Organismos del Estado, municipios, entidades descentralizadas y autónomas, así como cualquier persona que reciba fondos del Estado. Consecuentemente, es en virtud de tales normas por las que la Contraloría de Cuentas debe cumplir su función fiscalizadora en todo lo que involucre fondos del Estado, incluidos, los actos de enajenación de bienes nacionales, resultando antitécnico una norma específica en cada ley que se emita, que sería innecesaria por repetitiva.

3.2 Normas de auditoría gubernamental interna y externa

"Ley orgánica de la Contraloría General de Cuentas Decreto Número 31-2002 del Congreso de la República, le asigna la atribución de ser el órgano rector del control gubernamental; y, en ese contexto, es la única entidad responsable de implementar un sistema de auditoría del sector gubernamental". (6:3)

La vigencia de estos postulados se explica por sí sola, por cuanto el compromiso de contribuir al mejoramiento de la administración financiera del Estado, por medio de un trabajo profesional e independiente, es una obligación institucional que, de hecho, impulsa y provoca credibilidad tanto de la ciudadanía, como de las instituciones y los funcionarios que las dirigen.

Los constantes cambios en el ambiente gubernamental, exigen una acción fiscalizadora calificada y consistente con los avances tecnológicos y la aplicación de diferentes tendencias y filosofías que promueven cambios constantes en los entes públicos; en tal sentido, la Contraloría General de Cuentas, puso en vigencia las Normas de Auditoría para el sector Gubernamental, quedando como una responsabilidad permanente el contribuir, por medio de sus autoridades y

auditores gubernamentales, internos y externos, para que las Normas de Auditoría Gubernamental sean aplicadas y actualizadas oportunamente por el ente fiscalizador antes mencionado, como un medio de retroalimentación para que los sistemas sean evaluados en todas las entidades públicas y funcionen en forma eficiente, para que la gestión institucional sea más productiva, de tal manera que se manifieste el valor agregado de la profesión.

La aplicación de dichas normas, contribuirá a que los trabajos de Auditoría del sector gubernamental, se encuentren dentro de un contexto moderno bajo estándares exigidos por el ambiente cambiante de la administración pública, así como congruente con los sistemas integrados de administración y finanzas, y con otros procedimientos que utilizan las instituciones en su diario ejercicio operacional, en procura de alcanzar sus objetivos en forma eficiente, efectiva y económica.

3.2.1 Normas de auditoría para el sector gubernamental

Son el elemento básico que fija las pautas técnicas y metodológicas de la auditoría gubernamental, porque ayudan a desarrollar adecuadamente un proceso de auditoría con las características técnicas.

Constituyen un medio técnico para fortalecer y estandarizar el ejercicio profesional del auditor gubernamental y permiten la evaluación del desarrollo y resultado de su trabajo.

"Las normas de auditoría del sector gubernamental, son de cumplimiento obligatorio por parte de todos los auditores que ejecuten auditorías de carácter interno y externo en todas las entidades del sector público guatemalteco; asimismo, son de observancia general para las firmas privadas de auditoría, profesionales y especialistas de otras disciplinas que participen en el proceso de la auditoría gubernamental". (9:3)

Las normas de auditoría para el sector gubernamental se clasifican en cinco grupos:

- Normas personales.
- Normas para la planificación de la auditoría gubernamental.
- Normas para la ejecución de la auditoría gubernamental.
- Normas para la comunicación de resultados.
- Normas para el aseguramiento de calidad.

3.2.1.1 Normas personales

"Se refieren a los requisitos técnicos, personales y profesionales que debe reunir el auditor del sector gubernamental". (9:3)

Las normas personales se refieren a:

- Capacidad técnica y profesional.
- Independencia.
- Cuidado y esmero profesional.
- Confidencialidad y objetividad.

Si bien las normas personales son de importancia, ya que son parte del marco regulatorio de la Contraloría General de Cuentas, ente fiscalizador gubernamental de Guatemala, no se detallaran debido a que no son determinantes para la realización de la presente investigación.

3.2.1.2 Normas para la planificación de la auditoría del sector gubernamental

La planificación consiste en desarrollar una estrategia de auditoría, que permita adoptar decisiones apropiadas acerca de la naturaleza, oportunidad y alcance del trabajo de auditoría gubernamental, así como identificar lo que se debe hacer, por quién y cuándo.

"Las normas para el proceso de planificación de la auditoría se dividen en: Plan Anual de Auditoría Gubernamental y Planificación Específica de la Auditoría". (9:5)

a. Plan anual de auditoría gubernamental

"La Contraloría General de Cuentas y las unidades de Auditoría Interna del sector gubernamental definirán, dentro de sus actividades generales para cada ejercicio fiscal, un Plan Anual de Auditoría Gubernamental". (9:5)

b. Planificación específica de la auditoría

"El trabajo del auditor del sector gubernamental debe ser adecuadamente planificado, para contribuir a realizar auditorías de alta calidad, con base en el conocimiento general de las actividades que desarrolla la entidad auditada, así como los factores que la afecten". (9:5)

La planificación específica de una auditoría, implica desarrollar una estrategia para la ejecución del trabajo, a fin de asegurar que el auditor del sector gubernamental tenga un conocimiento adecuado de la entidad a auditar, que le permita evaluar el nivel de riesgo de la auditoría, así como determinar y programar la naturaleza, oportunidad y alcance de los procedimientos a aplicar.

La planificación específica se divide en:

- "Familiarización con el ente a auditar: comprende el conocimiento general de la entidad y el área objeto de examen, a través de la revisión del archivo permanente, los sistemas de información y los procesos operacionales.
- Evaluación preliminar del control interno: la evaluación preliminar es un procedimiento necesario para identificar las posibles áreas críticas, y definir la naturaleza, oportunidad y alcance de los procedimientos de auditoría.
- Elaboración del memorando de planificación: este documento es el resultado del trabajo efectuado durante la familiarización y evaluación preliminar del control interno. El memorando de planificación resume los criterios a ser utilizados por el auditor del sector gubernamental, y sirve de base para definir los objetivos generales y específicos, naturaleza y alcance del trabajo y la estimación de recursos y tiempo necesario.
- Elaboración de los programas de auditoría: para el análisis de cada área seleccionada, se elaborarán los programas de auditoría respectivos, que

representan una relación ordenada de procedimientos a ser aplicados en el proceso de la auditoría, para obtener la evidencia suficiente, competente y pertinente para alcanzar los objetivos establecidos". (9:6)

c. Normas para la ejecución de la auditoría del sector gubernamental

"El objetivo principal es orientar la ejecución de la auditoría con base en la planificación específica, a través de la aplicación adecuada de técnicas y procedimientos que permitan obtener evidencia, suficiente, competente y pertinente, para cumplir con los objetivos de cada auditoría." (9:8)

Las normas para la ejecución de la auditoría se dividen en:

- "Estudio y evaluación del control interno: comprende la evaluación de la eficiencia y eficacia del ambiente y estructura de control interno establecido, para determinar su grado de confiabilidad y repercusión en los resultados de las operaciones y la razonabilidad de la información financiera y administrativa." (9:9)
- "Evaluación del cumplimiento de disposiciones legales y reglamentarias: en la ejecución de la auditoría del sector gubernamental debe evaluarse el cumplimiento de las leyes y reglamentos aplicables." (9:9)
- "Actualización del archivo permanente: todo auditor del sector gubernamental durante el proceso de la auditoría está obligado a actualizar el archivo permanente." (9:9)
- "Supervisión del trabajo de auditoría: el trabajo de auditoría debe ser apropiadamente supervisado a efecto de asegurar su calidad técnica y profesional para cumplir con los objetivos propuestos." (9:9)
- "Obtención de evidencia comprobatoria: el auditor del sector gubernamental debe obtener la evidencia necesaria que se ajuste a la naturaleza y objetivos del examen, mediante la aplicación de pruebas de cumplimiento y sustantivas que le permitan fundamentar razonablemente los juicios y conclusiones que formule respecto a la entidad auditada." (9:10)

- "Elaboración de papeles de trabajo: el auditor del sector gubernamental debe elaborar y organizar un registro completo y detallado de papeles de trabajo, sobre el proceso de auditoría y sus resultados." (9:11)
- "Propiedad y archivo de los papeles de trabajo: los papeles de trabajo son propiedad de la Contraloría General de Cuentas, de las unidades de auditoría interna de las entidades del sector público y de las firmas privadas de auditoría, deberán permanecer en el archivo de papeles de trabajo de la institución que corresponda por el tiempo que establece la ley." (9:11)
- "Corroboración de posibles hallazgos y recomendaciones: los posibles hallazgos identificados deben ser discutidos con los responsables del área evaluada, así como con el personal técnico para corroborar los mismos, ratificar las evidencias y establecer la viabilidad y aplicabilidad de las recomendaciones." (9:12)
- "Comunicación acciones legales y administrativas ante la identificación de hallazgos: durante el proceso de la auditoría, el auditor del sector gubernamental debe establecer las posibles acciones legales y administrativas que se deriven de los hallazgos identificados en la entidad examinada." (9:12)

d. Normas para la comunicación de resultados

"Establecen los criterios técnicos del contenido, elaboración y presentación del informe de auditoría del sector gubernamental, asegurando la uniformidad de su estructura, así como la exposición clara y precisa de los resultados." (9:13)

Las normas para la comunicación de resultados se dividen en:

- "Forma escrita: el auditor del sector gubernamental debe preparar informes de auditoría por escrito para comunicar los resultados de cada auditoría. Su preparación debe ser en lenguaje sencillo y fácilmente entendible, tratando los asuntos en forma concreta y concisa, lo que debe coincidir de manera exacta y objetiva con los hechos observados." (9:13)

- "Contenido: todo informe de auditoría del sector gubernamental debe ajustarse a la estructura y contenido definido en los manuales respectivos." (9:14)
- "Discusión: el contenido de cada informe de auditoría del sector gubernamental debe ser discutido con los responsables de la entidad o unidad administrativa auditada, para asegurar el cumplimiento de las recomendaciones." (9:14)
- "Oportunidad en la entrega del informe: todo informe de auditoría del sector gubernamental debe emitirse al finalizar el trabajo, según los plazos establecidos en el manual de auditoría." (9:14-15)
- "Aprobación y presentación: todo informe de auditoría gubernamental emitido debe ser aprobado y presentado oficialmente." (9:15)
- "Seguimiento del cumplimiento de recomendaciones: la Contraloría General de Cuentas y las unidades de auditoría interna de las entidades del sector público, periódicamente, realizarán el seguimiento del cumplimiento de las recomendaciones de los informes de auditoría emitidos." (9:15)

e. Normas para el aseguramiento de la calidad

"Estas normas aseguran que todos los productos o servicios que brinda la Contraloría General de Cuentas, y las unidades de Auditoría Interna del sector Gubernamental, sean sometidos a un proceso de control de calidad en todas sus etapas." (9:16)

Las normas para el aseguramiento de la calidad se dividen en:

- "Políticas de calidad la Contraloría General de Cuentas y las unidades de auditoría interna del sector gubernamental, diseñarán e implementarán políticas y procedimientos que aseguren que los productos o servicios que proporcionan a sus clientes internos y externos, posean el mejor estándar de calidad y satisfagan sus expectativas." (9:16)
- "Mejoramiento continuo: se refiere a que permanentemente se debe evaluar y mejorar las políticas y procedimientos para asegurar la calidad en todas sus acciones." (9:17)

- "Conciencia de calidad: se refiere a que los auditores gubernamentales deben conocer las políticas y aplicar los procedimientos establecidos para el mejoramiento." (9:17)
- "Apoyo externo a la calidad: se refiera a buscar el apoyo de otras entidades fiscalizadoras superiores y organismos internacionales para medir la confiabilidad y vigencia de los procesos de calidad." (9:18)

3.2.2 Normas generales de control interno gubernamental

Para cumplir sus atribuciones, la Contraloría General de Cuentas emitió el presente cuerpo de normas generales de control interno (NGCI).

La aplicación cuidadosa del documento antes descrito, contribuirá a que los entes públicos organicen sus procedimientos de trabajo para que se ejecute un proceso administrativo adecuado, y un mejor control e información de los resultados de las operaciones, en un contexto moderno y bajo estándares exigidos por el ambiente cambiante de la administración pública, así como de los sistemas integrados de administración y finanzas, y otros medios que utilizan las instituciones en su diario ejercicio operacional, en procura de alcanzar sus objetivos en forma eficiente, efectiva y económica.

La Contraloría General de Cuentas tiene la responsabilidad, como órgano rector del Sistema de Auditoria Gubernamental (SAG), de contribuir por medio de sus autoridades y auditores, para que las Normas Generales de Control Interno, sean aplicadas y actualizadas oportunamente, como un medio eficaz de retroalimentación, que permita y propicie que los sistemas sean eficientes en todas las instituciones públicas.

Las normas generales de control interno gubernamental, son el elemento básico que fija los criterios técnicos y metodológicos para diseñar, desarrollar e implementar los procedimientos para el control, registro, dirección, ejecución e información de las operaciones financieras, técnicas y administrativas del sector público. Constituyen un medio técnico para fortalecer y estandarizar la estructura y ambiente de control interno institucional. La Contraloría General de Cuentas

establece que son de cumplimiento obligatorio por parte de todos los entes públicos.

Las mismas se clasifican en:

- Normas de aplicación general
- Normas aplicables a los sistemas de administración general.
- Normas aplicables a la administración de personal.
- Normas aplicables al sistema de presupuesto público.
- Normas aplicables al sistema de contabilidad integrada gubernamental.
- Normas aplicables al sistema de tesorería.
- Normas aplicables al sistema de crédito público.

En el caso particular de las normas generales de control interno gubernamental, únicamente se desarrollara una breve descripción de las mismas, debido a que se aplican en la presente investigación generalidades de dichas normas.

3.2.2.1 Normas de aplicación general

Se refieren a los criterios técnicos y metodológicos aplicables a cualquier institución sujeta a la fiscalización de la Contraloría General de Cuentas, independientemente de su magnitud y de los sistemas en funcionamiento.

Las normas de aplicación general se refieren a:

- Filosofía de control interno: debe nacer de la misión y visión institucionales, así como de los estándares o valores corporativos, que regirán el ambiente de control interno y el comportamiento de los funcionarios y de los servidores públicos.
- Estructura de control interno: es responsabilidad de la máxima autoridad de cada entidad pública, diseñar e implantar una estructura efectiva de control interno, que promueva un ambiente óptimo de trabajo para alcanzar los objetivos institucionales.
- Rectoría del control interno: la Contraloría General de Cuentas es el órgano rector del control gubernamental y responsable de establecer las normas

generales de control interno las cuales son de observancia obligatoria para cada entidad pública.

- Funcionamiento de los sistemas: es responsabilidad de la máxima autoridad de cada entidad pública, emitir los reglamentos o normas específicas que regirán el funcionamiento de los sistemas operativos, de administración y finanzas.
- Separación de funciones: la máxima autoridad de cada entidad pública, delimitará cuidadosamente, las funciones de las unidades administrativas y sus servidores.
- Tipos de controles: la máxima autoridad de cada entidad pública, establecerá e implementará, con claridad, los diferentes tipos de control que se relacionan con los sistemas administrativos y financieros.
- Evaluación del control interno y archivos: el ambiente y estructura de control interno debe ser evaluado de manera continua.
- Creación y fortalecimiento de las unidades de auditoría interna: la autoridad superior es la responsable de crear y mantener en opimas condiciones las unidades de auditoría interna, para lo cual las dotara de recursos financieros, humanos, materiales y tecnológicos; dichas unidades podrán ser evaluadas por la Contraloría General de Cuentas a través de la unidad administrativa correspondiente.
- Instrucciones por escrito: la máxima autoridad de cada ente público debe establecer que todas instrucción que deba cumplirse dentro de su organización, sea por escrito y divulgada hasta los niveles necesarios.
- Manuales de funcionamiento y procedimiento: la máxima autoridad de cada ente público debe apoyar y promover la elaboración de manuales de funciones y procedimientos que regulen el accionar de cada dependencia bajo su línea jerárquica.
- Archivos: cada entidad deberá velar por que sus archivos estén organizados de una forma lógica que permita localizar la información de manera fácil.

3.3 Normas internacionales para el ejercicio profesional de la auditoría interna –NIEPAI-

La metodología para realizar auditorías de tecnologías de la información, se conforma por la planificación, ejecución y la entrega del informe; debido a que existen diferentes marcos que brindan una guía para estos procesos. El marco del que se realiza referencia es el de las **normas internacionales para el ejercicio profesional de la auditoría interna,** que brinda el instituto de auditores internos (IIA, por sus siglas en ingles).

Las Normas se dividen en:

a) Normas sobre atributos: tratan sobre las características de las entidades y los individuos que desarrollan actividades de auditoría interna.

b) Normas sobre desempeño: describen la naturaleza de las actividades de auditoria interna y proveen criterio de calidad contra los cuales puede medirse la práctica de estos servicios.

c) Normas de implementación: estas son aplicables a tipos específicos de trabajo.

Los estándares de auditoría definen requerimientos obligatorios para la práctica de auditoría interna y presentación de informes que se detallan a continuación:

Estándar IIA 2110 Gobierno

La actividad de auditoría interna debe evaluar y hacer las recomendaciones apropiadas para mejorar el proceso de gobierno en el cumplimiento de los siguientes objetivos:

- Promover la ética y los valores apropiados dentro de la organización,
- Asegurar la gestión y responsabilidad eficaces en el desempeño de la organización,
- Comunicar la información de riesgo y control a las áreas adecuadas de la organización, y

- Coordinar las actividades y la información de comunicación entre el consejo de administración, los auditores internos y externos, y la dirección.

Estándar IIA 2110.A1 - La actividad de auditoría interna debe evaluar el diseño, implantación y eficacia de los objetivos, programas y actividades de la organización relacionados con la ética.

Estándar IIA 2110-A2 – La actividad de auditoría interna debe evaluar si el gobierno de tecnología de la información de la organización sostiene y apoya las estrategias y objetivos de la organización.

Para una adecuada ejecución de auditoría de tecnologías de la información el instituto de auditores internos, indica que deben considerarse como mínimo los siguientes aspectos contenidos en la clasificación de las normas sobre desempeño:

- Objetivos
- Alcance
- Evaluación de riesgos
- Cumplimiento de normas de auditoría, políticas y leyes aplicables
- Requerimientos de información y documentación
- Cronograma
- Producto a entregar

Estándar IIA 2200 - Planificación del trabajo

Los auditores internos deben desarrollar y documentar un plan para cada trabajo, incluyendo los objetivos del trabajo, el alcance, los plazos y la asignación de recursos.

Estándar IIA 2201 - Consideraciones de diseño

En la planificación del trabajo, los auditores internos deben tener en cuenta:

- Los objetivos de la actividad que está siendo revisada y los medios por los cuales la actividad controla su desempeño;

- Los riesgos significativos de la actividad, sus objetivos, los recursos, y las operaciones y los medios por los cuales el impacto potencial del riesgo se mantiene a un nivel aceptable;
- La idoneidad y eficacia de los procesos de gestión y control de riesgos de la actividad comparados con un cuadro de control correspondiente o modelo; y
- Las oportunidades para introducir mejoras significativas en los procesos de gestión de riesgos y control de la actividad.

Estándar IIA 2201.A1: al planear, los auditores internos deben establecer un acuerdo escrito acerca de los objetivos, el alcance, las responsabilidades respectivas y otras expectativas, incluidas las restricciones en la distribución de los resultados de la participación y el acceso a los registros.

Estándar IIA 2201.C1: los auditores internos deben establecer un entendimiento con los clientes del trabajo de consultar acerca de los objetivos, el alcance, las responsabilidades respectivas, y otras expectativas de los clientes. Para encargos importantes, este entendimiento debe ser documentado.

Estándar IIA 2210 - Los objetivos del trabajo

Los objetivos de los trabajos de consultoría deben considerar los procesos de gobierno, riesgo y control, hasta el grado de extensión acordado con el cliente.

Estándar IIA 2210.A1: los auditores internos deben realizar una evaluación preliminar de los riesgos relevantes de la actividad bajo revisión. Los objetivos del trabajo deben reflejar los resultados de esta evaluación.

Estándar IIA 2210.A2- los auditores internos deben considerar la probabilidad de errores significativos, fraude, incumplimiento y otras exposiciones en el desarrollo de los objetivos del trabajo.

Estándar IIA 2210.A3- se necesitan criterios adecuados para evaluar los controles. Los auditores internos deben determinar el grado en que la administración establece criterios adecuados para determinar si los objetivos y metas se logran.

Los auditores internos deben utilizar dichos criterios en su evaluación. Si no fuera apropiado, los auditores internos deben trabajar con la administración para desarrollar criterios de evaluación adecuados.

Estándar IIA 2210.C1: los objetivos del trabajo deben abordar la gobernabilidad, gestión de riesgos y control de procesos en la medida acordada con el cliente.

Estándar IIA 2210.C2: los objetivos del trabajo debe ser coherente con los valores, estrategias y objetivos de la organización.

Estándar IIA 2220 - Alcance del trabajo

Durante los trabajos de consultoría los auditores internos deben considerar los controles consistentes con los objetivos del trabajo y estar alertas a los asuntos de control significativos.

Estándar IIA 2220.A1: el alcance del trabajo debe incluir la consideración de los sistemas pertinentes, registros, al personal y las propiedades físicas, incluyendo aquellos bajo el control de terceros.

Estándar IIA 2220.A2: si surgen oportunidades de consultoría significativas durante un compromiso de aseguramiento, un acuerdo escrito específico en cuanto a los objetivos, el alcance, las responsabilidades respectivas y otras expectativas debe alcanzarse y los resultados del trabajo de consultoría transmitida de conformidad con las normas de consultoría.

Estándar IIA 2220.C1: en la realización de los trabajos de consultoría, los auditores internos deben asegurarse de que el alcance del trabajo es suficiente para hacer frente a la de los objetivos acordados. Si los auditores internos desarrollan sus reservas sobre el alcance durante el trabajo, estas reservas deben ser discutidas con el cliente para determinar si se debe continuar con el compromiso.

Estándar IIA 2220.C2: durante los trabajos de consultoría, los auditores internos deben abordar los controles en consonancia con los objetivos del trabajo y estar alerta a los problemas de control significativas.

Estándar IIA 2230 - Asignación de recursos para el trabajo

Los auditores internos deben determinar los recursos adecuados y suficientes para lograr los objetivos del trabajo sobre la base de una evaluación de la naturaleza y complejidad de cada tarea, las limitaciones de tiempo y los recursos disponibles.

Estándar IIA 2240 - Programa de trabajo de compromiso

Los auditores internos deben desarrollar y programas de trabajo de documentos que permitan alcanzar los objetivos del trabajo.

Estándar IIA 2240.A1: los programas de trabajo deben incluir los procedimientos para identificar, analizar, evaluar y documentar la información durante el trabajo. El programa de trabajo debe ser aprobado antes de su aplicación, y cualquier ajuste aprobado con prontitud.

Estándar IIA 2240.C1: los programas de trabajo para los trabajos de consultoría pueden variar en forma y contenido dependiendo de la naturaleza del trabajo.

Estándar IIA 2300 - Realización del compromiso

Los auditores internos deben identificar, analizar, evaluar y documentar la información suficiente para lograr los objetivos del trabajo.

Estándar IIA 2310 - Información de identificación

Los auditores internos deben identificar información suficiente, confiable, relevante y útil de información para alcanzar los objetivos del trabajo

Estándar IIA 2320 - Análisis y evaluación

Los auditores internos deben basar conclusiones y los resultados del trabajo en adecuados análisis y evaluaciones.

Estándar IIA 2330 – Información y documentación

Los auditores internos deben documentar información relevante para apoyar las conclusiones y los resultados del trabajo.

Estándar IIA 2330.A1: el director ejecutivo de auditoría debe controlar el acceso a los registros. El director ejecutivo de auditoría debe obtener la aprobación de la alta dirección y / o asesor legal antes de dar a conocer tales registros a terceros, según corresponda.

Estándar IIA 2330.A2: el director ejecutivo de auditoría debe establecer requisitos de custodia para los registros del trabajo, independientemente del medio en el que se almacena cada registro. Estos requisitos de retención deben ser coherentes con las directrices de la organización y cualquier regulación pertinente u otros.

Estándar IIA 2330.C1: el director ejecutivo de auditoría debe desarrollar políticas que rigen la custodia y retención de consultar los registros del trabajo, así como su puesta en libertad a las partes internas y externas. Estas políticas deben ser coherentes con las directrices de la organización y cualquier regulación pertinente u otros.

Estándar IIA 2340 - Supervisión del trabajo

Los compromisos deben ser supervisados adecuadamente para garantizar la consecución de sus objetivos, la calidad y el desarrollo del personal.

Estándar IIA 2400 - Comunicación y Resultados

Los auditores internos deben comunicar los resultados de los trabajos.

Estándar IIA 2410 - Criterios para la comunicación

Las comunicaciones deben incluir los objetivos y alcance del trabajo, así como las conclusiones correspondientes, las recomendaciones y planes de acción.

Estándar IIA 2410.A1: la comunicación final de los resultados del trabajo debe, en su caso, contener opinión y / o conclusiones de los auditores internos. Una vez expedida una opinión o conclusión ha de tener en cuenta las expectativas de la alta dirección, la junta, y otras partes interesadas y deben ser respaldadas por información suficiente, confiable, relevante y útil.

Estándar IIA 2410.A2: se anima a los auditores internos reconocer un rendimiento satisfactorio en las comunicaciones del trabajo.

Estándar IIA 2410.A3: al liberar a los resultados del trabajo ajenos a la organización, la comunicación debe incluir limitaciones a la distribución y uso de los resultados.

Estándar IIA 2410.C1: comunicación de los avances y resultados de los trabajos de consultoría varían en forma y contenido dependiendo de la naturaleza del trabajo y las necesidades del cliente.

Estándar IIA 2420 - Calidad de las comunicaciones

Las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas.

Estándar IIA 2440 - Difusión de resultados

El director ejecutivo de auditoría debe comunicar los resultados a las partes interesadas.

Estándar IIA 2440.A1: el director ejecutivo de auditoría es responsable de comunicar los resultados finales a las partes que puedan asegurar que los resultados se dan la debida consideración.

Estándar IIA 2440.C2: durante los trabajos de consultoría, gobierno, gestión de riesgos y problemas de control pueden ser identificados. Siempre que estas cuestiones son importantes para la organización, deben ser comunicados a la alta dirección y el consejo.

Estándar IIA 2450 - Opiniones globales

Cuando se emiten opiniones globales, debe considerar las expectativas de la alta dirección, el consejo y otras partes interesadas y debe ser soportada por información suficiente, fiable, relevante y útil.

3.4 Comité Patrocinador de Organizaciones -COSO-

El Comité Patrocinador de Organizaciones por sus siglas en inglés -COSO-, se constituyó en 1985 para formar la Comisión Nacional de Información Financiera Fraudulenta, una iniciativa independiente del sector privado que estudia los factores causales que pueden conducir a la información financiera fraudulenta.

Con respecto al control interno, en 1992, se publicó el Marco Integrado Control Interno (Informe COSO), este marco fue revisado y reeditado en mayo de 2013.

3.4.1 Marco Integrado de Control Interno 1992

"El Marco Integrado Control Interno emitido en el año de 1992, denominado los Nuevos Conceptos del Control Interno (Informe COSO), contiene la definición del control Interno y lo define como: un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos; así mismo, se puede encontrar los componentes y objetivos del control interno que relacionan a las unidades o actividades de la entidad que relacionadas entre sí, conforman una matriz tridimensional en forma de cubo, como se puede observar a continuación:

Dentro de los componentes de control interno, específicamente los tipos de actividades de control, se encuentran el proceso de información y los controles

sobre los sistemas de información, se conforman en dos categorías por controles generales y controles de aplicación". (5:15)

Controles Generales

Los controles generales o controles de la tecnología de la información son los relacionados a la gestión de la seguridad del centro de datos, la adquisición y mantenimiento de software, el control de acceso y el desarrollo y mantenimiento de las aplicaciones. Los que se amplían a continuación:

- **Controles sobre las operaciones del centro de proceso de datos**

Estos controles incluyen la organización y la planificación de las asignaciones, los usuarios orientados a procesar, almacenar y consultar información, los planes de recuperación de servicios informáticos.

- **Controles sobre el software**

Son los controles sobre la adquisición, la implementación, y el mantenimiento del software necesario para el funcionamiento del conjunto del sistema y la ejecución de las aplicaciones: sistemas de explotación, sistemas de gestión de bases de datos, software de telecomunicaciones, de seguridad y utilidades.

- **Controles sobre la seguridad de acceso**

Son los que permiten proteger el sistema contra el acceso, el uso no autorizado, y prevenir la piratería informática.

- **Controles sobre el desarrollo y mantenimiento de las aplicaciones**

La metodología para el desarrollo de aplicaciones que permite ejercer un control para el diseño y la implementación de sistemas de información, poniendo especial énfasis en las fases específicas, las necesidades de documentación de los distintos proyectos.

- **Controles de aplicación**

Los controles de aplicación, como su nombre indica, están diseñados para controlar el funcionamiento de las aplicaciones. Permite asegurar la totalidad y exactitud en el proceso de transacciones, su autorización y validez.

Estos controles son capaces de evitar que se introduzcan errores en el sistema, además de detectarlos y corregirlos una vez dentro, como comprobaciones de edición informatizadas, que consisten en comprobaciones de formato, existencia, razonabilidad de datos y otras comprobaciones que se incorporan en cada aplicación durante su desarrollo.

- **Medición y evaluación de riesgos**

Se debe estimar la frecuencia con que se presentarán los riesgos identificados, así como también se debe cuantificar la probable pérdida que ellos pueden ocasionar. Una vez identificados los riegos a nivel de organismo y de programa/actividad, debe procederse a su análisis. Los métodos utilizados para determinar la importancia relativa de los riesgos pueden ser diversos e incluirán como mínimo una estimación de su importancia, la evaluación de su probabilidad de ocurrencia y la valoración de la pérdida que podría provocar en caso de materializarse. Para determinar el orden de importancia general de los riesgos es necesario considerar su frecuencia y el impacto que pueden provocar en la organización. Con estas consideraciones podemos construir una matriz de riesgos que permitirá identificar los riesgos prioritarios.

3.5 Objetivos de control para información y tecnologías relacionadas (COBIT por sus siglas en ingles)

COBIT proviene de las siglas en inglés control objectives for information and related technology, marco de referencia emitido por la Asociación de Auditoría y Control de Sistemas de Información, por sus siglas en inglés ISACA.

El marco de negocio para el gobierno y la gestión de las tecnologías de la información de la empresa COBIT, ayuda a las organizaciones a crear un valor

óptimo a partir de las tecnologías de la información, al mantener un equilibrio entre la realización de beneficios y la optimización de los niveles de riesgo y utilización de los recursos.

La que permite a las tecnologías de la información y relacionadas se gobiernen y administren de una manera eficiente y eficaz a nivel de toda la organización, incluyendo el alcance completo de todas las áreas de responsabilidad y de negocios, considerando los intereses relacionados con las tecnologías de la información de las partes interesadas internas y externas.

La información constituye un recurso clave para todas las organizaciones crea, usa, retiene y divulga.

La tecnología juega un papel clave en las actividades diarias, es parte integral de todos los aspectos de la vida personal y comercial.

Las organizaciones y sus ejecutivos realizan esfuerzos para mantener la información de calidad para apoyar las decisiones del negocio, generar un valor comercial de las inversiones habilitadas por la Tecnología de la Información, lograr metas estratégicas y mejoras al negocio mediante el uso eficaz e innovador de las tecnologías de la información.

Lograr una excelencia operativa mediante la aplicación eficiente y fiable de la tecnología, mantiene el riesgo relacionado con las tecnologías de la información a niveles aceptables, optimizar el costo de la tecnología y los servicios de las tecnologías de la información.

Para lograr valor para las partes interesadas de la organización, se requiere un buen gobierno y una buena administración de los activos de las tecnologías de la información, los directivos, gerentes y ejecutivos de las organizaciones deben acoger la tecnología de la información como cualquier otra parte importante del negocio.

Cada día aumentan y se complican más los requisitos externos, tanto legales como de cumplimiento regulatorio y contractual, relacionados con el uso de la

información y la tecnología en la organización, amenazando su patrimonio si no se cumplen.

A la fecha la herramienta publicada por ISACA, es COBIT5, la cual proporciona un marco integral, que ayuda a las organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la Organización.

3.5.1 COBIT 5 "Un marco de negocio para el gobierno y la gestión de las TI de la empresa"

"Une los cinco principios que permiten a la Organización construir un marco efectivo de Gobierno y Administración basado en una serie de eficacia y eficiencia de siete habilitadores, que optimizan la inversión en tecnología e información, así como su uso en beneficio de las partes interesadas." (11:5)

Los 5 Principios de COBIT 5:

1. Satisfacer las necesidades de las Partes Interesadas
2. Cubrir la Compañía de Forma Integral
3. Aplicar un solo Marco Integrado
4. Habilitar un Enfoque Holístico
5. Separar el Gobierno de la Administración

Los principios y habilitadores de COBIT 5 son genéricos y útiles para las organizaciones de cualquier tamaño, bien sean comerciales, sin fines de lucro o en el sector público.

3.5.1.1 Principio 1. Satisfacer las necesidades de las partes interesadas

Las organizaciones tienen muchas partes interesadas y crear valor significa cosas diferentes – a veces conflictivas – para cada una de ellas, en el Gobierno se trata de negociar y decidir entre los diversos intereses de beneficio de las diferentes partes interesadas. "El sistema de Gobierno deberá considerar a todas las partes interesadas al tomar decisiones con respecto a la evaluación de riesgos, los

beneficios y el manejo de recursos. Las compañías existen para crear valor para sus partes interesadas." (11:17)

Las necesidades de las partes interesadas deben ser transformadas en una estrategia accionable para la organización, las metas en cascada de COBIT 5 traducen las necesidades de las Partes Interesadas en metas específicas, accionables y personalizadas dentro del contexto de la organización, de las metas relacionadas con las tecnologías de la información y de las metas habilitadoras.

Permite definir las prioridades para implementar, mejorar y asegurar el gobierno corporativo de las tecnologías de la información, en base de los objetivos (estratégicos) de la organización y los riesgos relacionados, en la práctica, las metas en cascada: definen los objetivos y las metas tangibles y relevantes, en diferentes niveles de responsabilidad, filtran la base de conocimiento de COBIT 5, en base de las metas corporativas para extraer una orientación relevante para la inclusión en los proyectos específicos de implementación, mejora o aseguramiento y Claramente identifican y comunican qué importancia tienen los habilitadores (algunas veces muy operacionales) para lograr las metas corporativas.

3.5.1.2 Principio 2: Cubrir la empresa extremo-a-extremo

"Se concentra en el gobierno y la administración de la tecnología de la información y relacionadas desde una perspectiva integral a nivel de toda la Organización." (11:23)

Integra el gobierno de la tecnología de la información corporativa en el gobierno corporativo, o sea, el sistema de gobierno para la tecnología de la información corporativa propuesto por COBIT 5 se integra, de una manera fluida, en cualquier sistema de gobierno, toda vez que COBIT 5 está alineado a los últimos desarrollos en gobierno corporativo.

Cubre todas las funciones y los procesos dentro de la organización; COBIT 5 no solamente se concentra en la función de la tecnología de la información, sino trata

la tecnología de la información y relacionadas como activos que necesitan ser manejados como cualquier otro activo, por todos en la organización.

3.5.1.3 Principio 3: Aplicar un marco de referencia único integrado

"COBIT 5 está alineado con los últimos marcos y normas relevantes usados por las organizaciones:

- Gobierno Corporativo: COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000.
- Relacionado con Tecnologías de la Información: ISO/IEC 38500, ITIL, familia ISO/IEC 27000, entre otros.

Así se permite a la organización utilizar COBIT 5 como integrador macro en el marco de gobierno y administración." (11:25)

3.5.1.4 Principio 4: Hacer posible un enfoque holístico

"El enfoque holístico que realiza referencia COBIT 5 es relacionado a un gobierno y gestión de las tecnologías de información de la empresa efectivo y eficiente, conformado por factores que, individual y colectivamente, influyen sobre si algo funcionará en el caso de COBIT, Gobierno y Administración sobre la TI corporativa e impulsados por las metas en cascada, o sea: las metas de alto nivel relacionadas con la TI definen qué deberían lograr los diferentes habilitadores." (11:27)

Descritos por el marco de COBIT 5 en siete categorías.

1. Procesos: describen una serie organizada de prácticas y actividades para lograr determinados objetivos y producir una serie de resultados como apoyo al logro de las metas globales relacionadas con la TI.

2. Estructuras organizacionales: constituyen las entidades claves para la toma de decisiones en una organización.

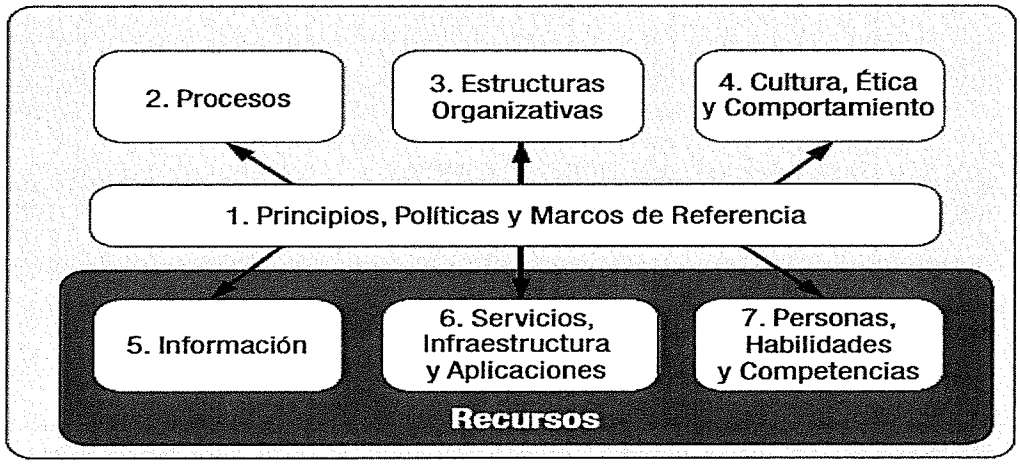
3. Cultura, ética y comportamiento: de los individuos, así como de la organización; se subestima frecuentemente como factor de éxito en las actividades de gobierno y administración.
4. Principios, políticas y marcos: son los vehículos para traducir el comportamiento deseado en una orientación práctica para la administración diaria.

5. Información: se encuentra presente en todo el ambiente de cualquier organización; o sea se trata de toda la información producida y usada por la Organización. La información es requerida para mantener la organización andando y bien gobernada, pero a nivel operativo, la información frecuentemente es el producto clave de la organización en sí.
6. Servicios, infraestructura y aplicaciones: incluyen la infraestructura, la tecnología y las aplicaciones que proporcionan servicios y procesamiento de tecnología de la información a la organización.

7. Personas, habilidades y competencias: están vinculadas con las personas y son requeridas para completar exitosamente todas las actividades y para tomar las decisiones correctas, así como para llevar a cabo las acciones correctivas.

Figura 2

Catalizadores corporativos de COBIT 5



Fuente: COBIT 5, ISACA.

Administración y Gobierno sistémico mediante habilitadores interconectados, para lograr los objetivos principales de la Organización, siempre debe considerarse una serie interconectada de habilitadores, o sea, cada habilitador necesita una entrada de otros habilitadores para ser completamente efectivo, o sea, los procesos necesitan información, las estructuras organizacionales necesitan habilidades y comportamiento y entrega un producto de salida a beneficio de otros habilitadores, o sea, los procesos entregan información, las habilidades y el comportamiento hacen que los procesos sean eficientes.

Esto constituye un principio clave que surge del trabajo de desarrollo de ISACA en el modelo de negocios para la seguridad de la información (BMIS por su sigla en inglés).

Las Dimensiones Habilitadores de COBIT 5:

1. Todos los habilitadores tienen una serie de dimensiones comunes. Dicha serie de dimensiones comunes.
2. Proporciona una manera común, sencilla y estructurada para tratar los habilitadores.
3. Permite a una entidad manejar sus interacciones complejas.
4. Facilita resultados exitosos de los habilitadores.

3.5.1.5 Principio 5: Separar el Gobierno de la Gestión

"Separar el gobierno de la administración el marco de COBIT 5 presenta una distinción muy clara entre el gobierno y la administración, las dos disciplinas comprenden diferentes tipos de actividades, requieren diferentes estructuras organizacionales y cumplen diferentes propósitos". (11:31)

Gobierno: en la mayoría de las organizaciones el Gobierno es responsabilidad de la Junta Directiva bajo el liderazgo de su presidente, asegura que se evalúen las necesidades de las partes interesadas, así como las condiciones y opciones, para determinar los objetivos corporativos balanceados acordados a lograr; fijando directivas al establecer prioridades y tomar decisiones; así como monitorear el

desempeño, cumplimiento y progreso comparándolos contra las directivas y objetivos fijados

Administración: en la mayoría de las organizaciones, la administración es responsabilidad de la gerencia ejecutiva, bajo el liderazgo del gerente general, planifica, construye, ejecuta y monitorea las actividades conforme a las directivas fijadas por el ente de Gobierno para lograr los objetivos de la Compañía.

COBIT 5 no es de uso obligatorio, pero propone que las organizaciones implementen los procesos de gobierno y administración de tal manera que las áreas claves queden cubiertas.

Los 37 procesos que contiene COBIT 5 se detallan a continuación

Procesos de gobierno de tecnología de la información empresarial

- **Evaluación, orientar y supervisar**

EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno.

EDM02 Asegurar la entrega de beneficios.

EDM03 Asegurar la optimización del riesgo.

EDM04 Asegurar la optimización de los recursos.

EDM05 Asegurar la transparencia hacia las partes interesadas.

Procesos para la gestión de la TI empresarial.

- **Alinear, planificar y organizar**

APO01 Gestionar el marco de gestión de TI.

APO02 Gestionar la estrategia.

APO03 Gestionar la arquitectura empresarial.

APO04 Gestionar la innovación.

APO05 Gestionar portafolio.

APO06 Gestionar el presupuesto y los costes.

APO07 Gestionar los recursos humanos.

APO08 Gestionar las relaciones.

APO09 Gestionar los acuerdos de servicio.

APO10 Gestionar los proveedores.

APO11 Gestionar la calidad.

APO12 Gestionar el riesgo.

APO13 Gestionar la seguridad.

- **Construir, adquirir e implementar**

BAI01 Gestionar los programas y proyectos.

BAI02 Gestionar la definición de requisitos.

BAI03 Gestionar la identificación y la construcción de soluciones.

BAI04 Gestionar la disponibilidad y la capacidad.

BAI05 Gestionar la introducción de cambios organizativos.

BAI06 Gestionar los cambios.

BAI07 Gestionar la aceptación del cambio y de la transición.

BAI08 Gestionar el conocimiento.

BAI09 Gestionar los activos.

BAI10 Gestionar la configuración.

- **Entregar, dar servicio y soporte**

DSS01 Gestionar las operaciones.

DSS02 Gestionar las peticiones y los incidentes del servicio.

DSS03 Gestionar los problemas.

DSS04 Gestionar la continuidad.

DSS05 Gestionar los servicios de seguridad.

DSS06 Gestionar los controles de los procesos del negocio.

- **Supervisar, evaluar y valorar**

MEA01 Supervisar, evaluar y valorar rendimiento y conformidad.

MEA02 Supervisar, evaluar y valorar el sistema de control interno.

MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

3.6 ISO 38500

Organización internacional de estándares (ISO, por sus siglas en inglés) es una organización internacional independiente, no gubernamental, con una membresía de 161 organismos nacionales de normalización. Por medio de sus miembros, que reúne a expertos para compartir conocimientos y desarrollar estrategias basadas en el consenso, el mercado normas internacionales voluntarias y relevantes que apoyan la innovación y aportar soluciones a los retos globales.

La norma ISO 38500 fue publicada en junio del 2008 como la primera de esta línea para el buen gobierno de las tecnologías de la información, basada en la norma australiana AS8015 de 2005. Su objetivo es proporcionar un marco de principios para que la dirección de las organizaciones los utilicen para evaluar, dirigir y monitorear el uso de las tecnologías de la información (TI's). Está alineada con los principios de gobierno corporativo recogidos en el "Informe Cadbury" y con

los "principios de gobierno corporativo de la organización para la cooperación y el desarrollo económicos". (17)

Es un estándar internacional que provee directrices para el gobierno corporativo de tecnologías de la información y ayuda a los miembros de altos niveles de una organización a entender y cumplir sus obligaciones legales, regulatorias y éticas respecto del uso de tecnologías de la información en las organizaciones.

Esta norma define el buen gobierno de las tecnologías de la información como el sistema usado por la alta dirección de la organización para controlar el uso presente y futuro de las tecnologías de la información en la organización, de manera que se consigan los planes y objetivos de la misma.

ISO/IEC 38500, como la mayoría de las normas de gestión ISO, es aplicable a entidades de todos los tamaños y sectores, incluidas las empresas públicas y privadas, administraciones públicas y otras.

La ISO/IEC 38500 completa otros estándares de gestión de tecnologías de la información, tales como la ISO 27001 y la ISO 20000, añadiendo una capa de gestión superior, estratégica a la que contemplan estas normas, cuyo enfoque es más operativo.
La Norma se basa en que la alta dirección evalúe, dirija y siga el uso que se hace de las tecnologías de la información en sus organizaciones de manera que se puedan obtener los siguientes resultados:

- Si la norma es seguida de manera adecuada, las partes implicadas (directivos, consultores, ingenieros, proveedores de hardware, auditores, etc.), puedan confiar en el gobierno corporativo de tecnologías de la información.
- Existan canales apropiados para informar y orientar a los directores que controlan el uso de las tecnologías de la información en su organización.
  Exista una base para la evaluación objetiva por parte de la alta dirección de la gestión de las tecnologías de información. Para conseguirlo, la norma

establece los seis principios básicos para el buen gobierno de las tecnologías de la información.

- Responsabilidad: asignar responsabilidades a personas competentes y con autoridad para tomar decisiones.
- Estrategia: alinear las actividades de tecnologías de la información con los objetivos de negocio, buscando el beneficio de la organización y asegurarse de que se obtiene dicho beneficio.
- Adquisición: invertir en tecnologías de la información de manera eficiente.
- Rendimiento: proporcionar la capacidad de tecnologías de la información necesaria para que el negocio funcione adecuadamente, se gestionen los riesgos y se protejan los recursos, midiendo cómo las tecnologías de la información presta soporte al negocio.
- Conformidad: proporcionar control interno suficiente para garantizar la conformidad legal o normativa de los sistemas de tecnologías de la información.
- Conducta humana: identificar el comportamiento humano que se requiere y desarrollar métodos de trabajo para utilizar las tecnologías de la información de manera apropiada.

3.6.1 Objetivos de la norma ISO 38500

"Asegurar a las partes interesadas (incluidos los consumidores, accionistas, y empleados) que, si se sigue la norma:

a) Pueden tener confianza en el gobierno corporativo de las tecnologías de la información de la organización.
b) Informar y guiar a los directores en el gobierno de la tecnología de la información en su organización.
c) Proporcionar una base para la evaluación objetiva del gobierno corporativo de las tecnologías de la información." (17)

3.6.1.1 Principios de la norma ISO 38500

"La norma define seis principios de un buen gobierno corporativo de las tecnologías de la información:

1. **Responsabilidad:** todo el mundo debe comprender y aceptar sus responsabilidades en la oferta o demanda de tecnologías de la información. La responsabilidad sobre una acción lleva aparejada la autoridad para su realización.
2. **Estrategia:** la estrategia de negocio de la organización tiene en cuenta las capacidades actuales y futuras de las tecnologías de la información. Los planes estratégicos de tecnologías de la información satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio.
3. **Adquisición:** las adquisiciones de tecnologías de la información se hacen por razones válidas, basándose en un análisis apropiado y continuo, con decisiones claras y transparentes. Hay un equilibrio adecuado entre beneficios, oportunidades, costes y riesgos tanto a corto como a largo plazo.
4. **Rendimiento:** las tecnologías de la información está dimensionada para dar soporte a la organización, proporcionando los servicios con la calidad adecuada para cumplir con las necesidades actuales y futuras.
5. **Conformidad:** la función de tecnologías de la información cumple todas las legislaciones y normas aplicables. Las políticas y prácticas al respecto están claramente definidas, implementadas y exigidas.
6. **Factor humano:** las políticas de TIC, prácticas y decisiones demuestran respecto al factor humano, incluyendo las necesidades actuales y emergentes de toda la gente involucrada." (17)

Para cada uno de los principios, la norma proporciona una breve guía u orientación sobre como evaluar, dirigir y monitorear la función de las tecnologías de la información. Son orientaciones muy generales que no incluyen mecanismos, técnicas o herramientas concretas a utilizar, cabe pensar que en futuras normas complementarias se irán concretando estos aspectos.

3.6.1.2 Modelo gobierno de las tecnologías de la información según la norma ISO 38500

La dirección debe gobernar las tecnologías de la información mediante cuatro tareas principales:

1. **Evaluar:** examinar y juzgar el uso actual y futuro de las tecnologías de la información, incluyendo estrategias, propuestas y acuerdos de aprovisionamiento (internos y externos).
2. **Dirigir:** la preparación y ejecución de los planes y políticas, asignando las responsabilidades al efecto.
3. **Monitorizar:** mediante sistemas de medición, vigilar el rendimiento de las tecnologías de la información, asegurando que se ajusta a lo planificado.

3.6.1.3 Beneficios de la aplicación de la norma ISO 38500

"La norma se aplica al gobierno de los procesos de gestión de las tecnologías de la información, en todo tipo de organizaciones que utilicen las tecnologías de la información, facilitando unas bases para la evaluación objetiva de dicho gobierno." (17)

Dentro de los beneficios de un buen gobierno de las tecnologías de la información estaría la conformidad de la organización con:

- Los estándares de seguridad.
- Legislación de privacidad.
- Legislación sobre el spam.
- Legislación sobre prácticas comerciales.
- Derechos de propiedad intelectual, incluyendo acuerdos de licencia de software.
- Regulación medioambiental.
- Normativa de seguridad y salud laboral.
- Legislación sobre accesibilidad.
- Estándares de responsabilidad social.

También la búsqueda de un buen rendimiento de las tecnologías de la información mediante:

- Apropiada implementación y operación de los activos de las tecnologías de la información.
- Clarificación de las responsabilidades y rendición de cuentas en lograr los objetivos de la organización
- Continuidad y sostenibilidad del negocio
- Alineamiento de las tecnologías de la información con las necesidades del negocio
- Asignación eficiente de los recursos
- Innovación en servicios, mercados y negocios
- Buenas prácticas en las relaciones con los interesados
- Reducción de costes
- Materialización efectiva de los beneficios esperados de cada inversión en tecnologías de la información.

3.7 Norma ISO 27001:2005

"ISO 27001 en Guatemala conocida como COGUANOR NTG_UNIT_ISO_IEC_27001-2005 es otro de los temas recurrentes en el ambiente de la seguridad informática y, al igual que con otros conceptos, hay muchas confusiones e interpretaciones erróneas o incompletas de lo que es y, sobre todo, para qué sirve y por lo tanto un mejor uso de ISO-27001, para un mejor provecho de este estándar propuesto por ISO." (2:10)

La definición formal se refiere a: El estándar para la seguridad de la información ISO/IEC-27001 (Information technology – Security techniques – Information security management systems – Requirements) fue aprobado y publicado en 2005, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

3.7.1 Sistema de gestión de seguridad de la información

A diferencia de otros estándares que, desde un punto de vista simplificado, fueron conceptualizados como una simple lista de requisitos a cumplir, ISO-27001 se creó, teniendo en cuenta un proceso de seguridad de la información basado en el famoso ciclo de "Deming ciclo de mejora continua o ciclo PDCA (por las iniciales de Plan, Do, Check and Act), creando con ello lo que se llamó el Sistema de Gestión de la Seguridad de la Información (conocido en inglés como el ISMS, Information Security Management System)". (2:20)

Antes de revisar qué es un sistema de gestión de seguridad de la información, es importante definir "seguridad de la información". Aunque para muchos pareciera un concepto demasiado básico, que en algunas ocasiones no se tiene claro y por lo mismo se es reiterativo para despejar cualquier duda. Se define la seguridad de la información como el logro, gestión y mantenimiento de tres características elementales:

- **Confidencialidad:** la información sólo debe ser vista por aquellos que tienen permiso para ello, no debe poder ser accedida por alguien sin el permiso correspondiente.
- **Integridad:** la información podrá ser modificada solo por aquellos con derecho a cambiarla.
- **Disponibilidad:** La información deberá estar disponible en el momento en que los usuarios autorizados requieren acceder a ella.

Estas tres características forman la famosa "CIA", por las siglas en inglés de confidencialidad, integridad y disponibilidad: Confidentiality, Integrity y Availability. Aunque se piensa que la seguridad de la información debe incluir una cuarta característica llamada "no repudiación", que asegura que un cambio a la información no sea negado (o repudiado) por quien realizó dicho cambio.

Este estándar internacional adopta también el modelo "Plan-Do-Check-Act" (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS, y significa lo siguiente:

Plan: (Establecer el Sistema de gestión de seguridad de la información): Implica, establecer a política, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.

Do: (Implementar y operar el sistema de gestión de seguridad de la información): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.

Check: (Monitorizar y revisar el sistema de gestión de seguridad de la información): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.

Act: (Mantener y mejorar el sistema de gestión de seguridad de la información): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del sistema de gestión de seguridad de la información o cualquier otra información relevante para permitir la continua mejora del sistema de gestión de seguridad de la información.

La finalidad de la norma, es preservar la C.I.A. de la información estableciendo un sistema, formado por un conjunto de procesos, gente y tecnología, que analice los riesgos de la información y establezca medidas para eliminarlos o minimizarlos de manera recurrente mediante un ciclo de mejora continua, manteniendo siempre el control de los riesgos para saber en todo momento la postura de seguridad de la organización. Es precisamente este sistema el que recibe el nombre de Sistema de Gestión de Seguridad de la Información, que es el punto central de la norma pues básicamente nos exige que cada organización que cumpla con ISO-27001 lleve a cabo cuatro grandes actividades:

- Establecer el sistema.
- Implementar y operar el sistema.
- Mantener y mejorar el sistema.
- Monitorear y revisar el sistema.

Como puede verse, el espíritu de la norma no habla de una lista de medidas, llamadas controles, para preservar la C.I.A. de lo que habla es de cómo crear y operar el sistema. Las características fundamentales de ISO-27001, al igual que de otras normas y mejores prácticas, es la exigencia de crear el SGSI y dejar bajo su tutela el análisis, definición y aplicación de las medidas para preservar la seguridad de la información.

El objetivo fundamental de la norma es crear y mantener el sistema que, por su propio diseño, nos llevará a seleccionar y mejorar constantemente los controles a implantar.

Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un proceso. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

3.7.1.1 Aplicación de la norma ISO 27001

Principios generales para lograr una adecuada implementación:

- Sistema de gestión de seguridad de la información.
- Responsabilidades de la Administración
- Auditoría Interna del sistema de gestión de seguridad de la información.
- Administración de las revisiones del Sistema de gestión de seguridad de la información.
- Mejoras del sistema de gestión de seguridad de la información.

Cualquier exclusión a los controles detallados por la norma y denominados como necesarios para satisfacer los criterios de aceptación de riegos, debe ser justificada y se debe poner de manifiesto, o evidenciar claramente los criterios por los cuales este riesgo es asumido y aceptado. "En cualquier caso en el que un control sea excluido, la conformidad con este estándar internacional, no será aceptable, a menos que dicha exclusión no afecte a la capacidad y/o

responsabilidad de proveer seguridad a los requerimientos de información que se hayan determinado a través de la evaluación de riesgos, y sea a su vez aplicable a las regulaciones y legislación vigente." (2:30)

3.7.1.2 Requerimientos generales:

La organización, establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documentado SGSI en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos. Para este propósito esta norma, está basada en el modelo PDCA

- Control de documentos: todos los documentos requeridos por el SGSI serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:
  - Aprobar documentos y prioridades o clasificación de empleo.
  - Revisiones, actualizaciones y reprobaciones de documentos.
  - Asegurar que los cambios y las revisiones de documentos sean identificados.
  - Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
  - Asegurar que los documentos permanezcan legibles y fácilmente identificables.
  - Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
  - Asegurar que los documentos de origen externo sean identificados.
  - Asegurar el control de la distribución de documentos.
  - Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito

3.7.1.3 Responsabilidades de administración

La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del SGSI a través de:

- Establecimiento de la política del sistema de gestión de la seguridad de la información.
- Asegurar el establecimiento de los objetivos y planes del sistema de gestión de la seguridad de la información.
- Establecer roles y responsabilidades para la seguridad de la información.
- Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.
- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el sistema de gestión de la seguridad de la información.
- Decidir los criterios de aceptación de riesgos y los niveles del mismo.
- Asegurar que las auditorías internas del sistema de gestión de la seguridad de la información, sean conducidas y a su vez conduzcan a la administración para la revisión del sistema de gestión de la seguridad de la información.

3.7.1.4 Formación, preparación y competencia

La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el sistema de gestión de la seguridad de la información sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria.

- **Auditoría interna del sistema de gestión de la seguridad de la información:** la organización realizará auditorías internas al sistema de gestión de la seguridad de la información a intervalos planeados para

determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

- **Administración de las revisiones del sistema de gestión de la seguridad de la información:** las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el sistema de gestión de la seguridad de la información incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, serán claramente documentados.

3.7.1.5 Mejoras al sistema de gestión de la seguridad de la información

La organización deberá mejorar continuamente la eficiencia del sistema de gestión de la seguridad de la información a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración.

3.7.1.6 Acciones correctivas al sistema de gestión de la seguridad de la información

La organización llevará a cabo acciones para eliminar las causas que no estén en conformidad con los requerimientos del sistema de gestión de la seguridad de la información con el objetivo de evitar la recurrencia de los mismos.

3.8 Norma ISO 27002:2005

"La ISO 27002 es una guía de recomendaciones de buenas prácticas para la gestión de seguridad de la información .cubre no solo la problemática de las tecnologías de la información (information technology por sus siglas en inglés) sino que hace una aproximación holística a la seguridad corporativa de la información

extendiéndose a todas las funcionalidades de una organización en cuanto puedan afectar la seguridad de la información." (3:5)

Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

3.8.1 Evaluación de los riesgos de seguridad conforme a la Norma ISO 27002:2005

Las evaluaciones del riesgo debe identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización.

"La evaluación del riesgo debe incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo)." (3:17)

Las evaluaciones del riesgo también se debe realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se realizan de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de la evaluación del riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema o servicios donde esto es practicable, realista y útil. Tratamiento de los riesgos de seguridad conforme a la Norma ISO 27002:2005

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se evalúa que el riesgo es bajo o que el costo del

tratamiento no es efectivo en costo para la organización. Estas decisiones deben ser documentadas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

- Aplicar los controles apropiados para reducir los riesgos;
- Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;
- Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;
- Transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.

Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles deberán ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles deberán asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:

- Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:
- Objetivos organizacionales;
- Requerimientos y restricciones operacionales;
- Costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;
- La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o medio ambiente, y podría no ser practicable en todas las organizaciones. Como ejemplo, se pueden segregar las tareas para evitar el fraude y el error. En las organizaciones más pequeñas puede no ser posible segregar todas las tareas y pueden ser necesarias otras maneras para lograr el mismo objetivo de control. En otro ejemplo, describe cómo se debe monitorear el uso del sistema y recolectar la evidencia. Los controles descritos; por ejemplo, bitácora de eventos; podrían entrar en conflicto con la legislación aplicable, como la protección de la privacidad para los clientes o en el centro de trabajo.

Se debe considerar los controles de seguridad de la información en los sistemas y la especificación de los requerimientos de proyectos, así como la etapa de diseño. El no hacerlo puede resultar en costos adicionales y soluciones menos efectivas, y tal vez, en el peor de los casos, la incapacidad de lograr la seguridad adecuada.

Tener en mente que ningún conjunto de controles puede lograr la seguridad completa, y que implementar una acción de gestión adicional para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar los objetivos de la organización, no necesariamente implica una mejora del sistema.

3.8.1.1 Política de seguridad contenida en la Norma ISO 27002

"Política de seguridad de la información

Objetivo: proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

El documento de la política de seguridad de la información es aprobado por la gerencia, publicado y comunicado a todos los empleados y la población en general cuando así sea requerido.

La política de seguridad de la información debe ser revisada a intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad." (3:25)

Las actividades de la seguridad de la información deben ser coordinadas por representantes de diferentes partes de la organización con roles y funciones laborales relevantes.

Todas las responsabilidades de la seguridad de la información deben estar claramente definidas.

- Mantener contactos apropiados con grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales. Mejorar el conocimiento sobre las mejores prácticas y mantenerse al día con la información de seguridad relevante;
- Asegurar el entendimiento del ambiente de seguridad de la información sea actualizado y completo;
- Recibir advertencias tempranas de alertas, asesorías y avisos relacionados con ataques y vulnerabilidades.

Se identifican los riesgos para la información y los medios de procesamiento de la información de la organización a raíz de procesos comerciales que involucran a grupos externos y se debieran implementar controles apropiados antes de otorgarles acceso.

3.8.1.2 Gestión de activos

- **Responsabilidad por los activos**

Objetivo: lograr y mantener una apropiada protección de los activos organizacionales.

Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y se deben asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

- **Inventario de los activos**

Identificar todos los activos y se debe elaborar y mantener un inventario de todos los activos importantes.

Una organización identifica todos los activos y documenta la importancia de estos activos. El inventario de los activos incluirá toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. El inventario no duplica innecesariamente otros inventarios, pero se asegura la organización que el contenido esté alineado.

- **Propiedad de los activos**

El término propietario identifica una persona o entidad que cuenta con la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. (El término propietario no significa que la persona en realidad tenga algún derecho de propiedad sobre el activo).

Lineamiento de implementación

El propietario del activo debiera ser responsable de:

a) asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente;
b) definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.

La propiedad puede ser asignada a:

- Un proceso comercial;
- Un conjunto de actividades definido;
- Una aplicación; o
- Un conjunto de data definido.
- Otra información

Se pueden delegar las tareas rutinarias; por ejemplo, a un empleado que supervisa el activo diariamente, pero la responsabilidad permanece con el propietario.

En los sistemas de información complejos podría ser útil designar grupos de activos, los cuales actúan juntos para proporcionar una función particular como servicios. En este caso el propietario es responsable de la entrega del servicio, incluyendo el funcionamiento de los activos que los proveen.

- **Uso aceptable de los activos**: se deben identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.
- **Lineamiento de implementación**: todos los empleados, contratistas y terceros deberán seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información, incluyendo:

– reglas para la utilización del correo electrónico e Internet.
– lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización.

- **Etiquetado y manejo de la información**: desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización.

Lineamiento de implementación

Los procedimientos para el etiquetado de la información necesitan abarcar los activos de información en formatos físicos y electrónicos.

- **Seguridad de recursos humanos**

Objetivo: asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las responsabilidades de seguridad deben ser tratadas antes del empleo en descripciones de trabajo adecuadas y en los términos y condiciones del empleo.

Los antecedentes de todos los candidatos al empleo, contratistas y terceros debieran ser adecuadamente investigados, especialmente para los trabajos confidenciales.

Los empleados, contratistas y terceros usuarios de los medios de procesamiento de la información debieran firmar un acuerdo sobre sus roles y responsabilidades con relación a la seguridad.

- **Roles y responsabilidades**

Se deben definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización.

- **Lineamiento de implementación**

Los roles y responsabilidades deben incluir requerimientos para:

a) Implementar y actuar en concordancia con las políticas de seguridad de la información de la organización.
b) Proteger los activos contra el acceso, divulgación, modificación, destrucción o interferencia no autorizada;
c) Ejecutar procesos o actividades de seguridad particulares;

d) Asegurar que se asigne a la persona la responsabilidad por las acciones tomadas;
e) Reportar eventos de seguridad o eventos potenciales u otros riesgos de seguridad para la organización.

- **Términos y condiciones del empleo**

a) Control: Como parte de su obligación contractual; los usuarios empleados, contratistas y terceros deben aceptar y firmar un contrato con los términos y condiciones de su empleo, el cual establece sus responsabilidades y las de la organización para la seguridad de la información.

b) Durante el empleo: asegurar que los usuarios empleados, proveedores y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se definen las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona, dentro de la organización.

Se proporciona a todos los usuarios empleados, contratistas y terceras personas un nivel adecuado de conocimiento, educación y capacitación en procedimientos de seguridad y uso correcto de los medios de procesamiento de información para minimizar los posibles riesgos de seguridad. Se debiera establecer un proceso disciplinario normal para manejar las fallas en la seguridad.

- **Responsabilidades de la gerencia**

La gerencia debiera requerir a los usuarios empleados, contratistas y terceras personas que apliquen la seguridad en concordancia con políticas y procedimientos bien establecidos por la organización.

- **Conocimiento, educación y capacitación en seguridad de la información**

a) Control: todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas deben recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

b) Proceso disciplinario: Debe existir un proceso disciplinario para los empleados que han cometido un incumplimiento de la seguridad.

c) Lineamiento de implementación: el proceso disciplinario no debiera iniciarse sin una verificación previa de la ocurrencia del incumplimiento de la seguridad.

El proceso disciplinario formal debe asegurar el tratamiento correcto y justo para los empleados sospechosos de cometer incumplimientos de la seguridad. El proceso disciplinario proporciona una respuesta equilibrada que tome en consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en el negocio, si esta es la primera ofensa, si el culpable fue apropiadamente capacitado, la legislación relevante, contratos comerciales y otros factores que se puedan requerir. En los casos serios de dolo, el proceso permite la remoción inmediata de los derechos de acceso y privilegios, y si fuese necesario, acompañar inmediatamente a la personas fuera del local.

- **Gestión de claves**

Se establecerá la gestión de claves para dar soporte al uso de técnicas criptográficas en la organización.

a) **Lineamiento de implementación**: todas las claves criptográficas deben estar protegidas contra una modificación, pérdida y destrucción. Además, las claves secretas y privadas necesitan protección contra la divulgación

no-autorizada. Se debe proteger físicamente el equipo utilizado para generar, almacenar y archivar las claves.

b) **Seguridad de los archivos del sistema**: garantiza la seguridad de los archivos del sistema.

Se controlará el acceso a los archivos del sistema y el código fuente del programa, y los proyectos de tecnologías de la información y las actividades de soporte se realizaran de una manera segura.

c) **Control del software operacional**: se establecen procedimientos para el control de la instalación del software en los sistemas operacionales.

- **Lineamiento de implementación**: para minimizar el riesgo de corrupción de los sistemas operacionales, se debieran considerar los siguientes lineamientos para controlar los cambios:

I. La actualización del software operacional, aplicaciones y bibliotecas de programas sólo debe ser realizada por administradores capacitados con la apropiada autorización gerencial

II. Los sistemas operacionales sólo deben mantener códigos ejecutables aprobados, y no códigos de desarrollo o compiladores;

III. El software de las aplicaciones y el sistema de operación sólo se debe implementar después de una prueba extensa y satisfactoria; las pruebas incluyen pruebas de utilidad, seguridad, efectos sobre los sistemas y facilidad para el usuario; y se llevan a cabo en sistemas separados o paralelos;

IV. Se utiliza un sistema de control de configuración para mantener el control de todo el software implementado, así como la documentación del sistema;

V. Se establece una estrategia de regreso a la situación original (rollback), antes de implementar los cambios.

3.9 Norma ISO 27005:2005

Los riesgos debe ser una parte integral de todas las actividades de gestión de seguridad de la información pues en ellos son la principal herramienta para cubrir los requisitos de seguridad es por ello la importancia de la norma ISO 27005, donde esta norma puede ser implementada en una organización completa como si fuera un todo o también a solo una parte de ella, todo esto solo para evaluar el riego de cada aspecto y de esta manera tomar decisiones adecuada, lo cual se hace por medio de pasos primero está el Análisis de Riesgos el cual consta de identificación de riesgos y las fases de estimación los cuales tiene por objeto evaluar el nivel de riesgo, luego esta Evaluación de Riesgos para esto se hace un análisis de riesgos y las fases de evaluación lo cual se utilizan para tomar decisiones y tener en cuenta los objetivos de la organización el cual consiste en el tratamiento de riesgos y las fases de aceptación del riesgo esto es para reducir, retener, evitar o transferir los riesgos. "Comunicación de Riesgos donde se logra llegar a un acuerdo sobre la forma de gestionar los riesgos mediante el intercambio y/o compartir información acerca de los riesgos entre los tomadores de decisiones y otras partes interesadas y por ultimo tenemos La Vigilancia del Riesgo y la Revisión: para detectar oportunidades en el contexto de la organización en una etapa temprana, y para mantener una visión general de la instantánea completa del riesgo." (4:5)

Diseñada para ayudar a la aplicación satisfactoria de seguridad de la información, la necesidad de identificar la información activos en riesgo, las posibles amenazas o fuentes de amenaza, las potenciales vulnerabilidades y las posibles consecuencias (impactos) si los riesgos se materializan.

3.9.1 Seguridad de la información según Norma ISO 27005:2005

La información en todas sus formas (automatizada o no, formalizada o no, pública o reservada), es uno de los principales artefactos de cualquier tipo de organización, necesarios para el normal funcionamiento de los objetivo previstos a alcanzar.

Debido a esa importancia, las organizaciones necesitan proteger su información para garantizar que esté disponible cuando se necesite, este tema aparentemente puede ser una tarea fácil de llevar pero la realidad es otra, pues la cantidad de información que puede manejar una organización puede crecer de manera exponencial, lo que dificulta el trabajo para su protección.

Se entiende por Gestión de la seguridad de la información el proceso por el cual la organización define, alcanza y mantiene unos niveles apropiados de confiabilidad, integridad, disponibilidad, trazabilidad y autenticidad para la información que necesita operar.

3.9.2 Aspectos principales del proceso de gestión de la seguridad de la información según Norma ISO 27005:2005

El proceso de Gestión de la seguridad de la información incluye los siguientes aspectos principales:

- Determinar los objetivos, estrategias y políticas de seguridad de la información.
- Determinar los requerimientos de seguridad de la información.
- Identificar y analizar las amenazas y las vulnerabilidades de los activos de la información.
- Identificar y analizar los riesgos de seguridad.
- Asegurar la concienciación de todo el personal en materia de seguridad de la información.
- Detectar los posibles incidentes de seguridad y reaccionar ante ellos.

Además de los aspectos que se tienen en cuenta dentro del proceso de gestión de la seguridad de la información, es importante tener en cuenta algunos datos relevantes sobre la complejidad que puede alcanzar el proceso de gestión de la seguridad de la información en las organizaciones, dichos datos son:

- **Crecimiento de los incidentes provocados por el personal de la organización:** un volumen significativo de pérdidas se debe a debilidades

tecnológicas, como el robo o la pérdida de soportes de información o el abuso de privilegios por parte de usuarios de sistemas de información.

- **Ataques con motivación cien por ciento económica**: por lo anterior en los últimos años, la disciplina de seguridad de la información ha experimentado un rápido desarrollo, impulsada por la necesidad de formalizar todas las medidas de seguridad necesarias para proteger la información.

3.9.3 Análisis de riesgos basados en la Norma ISO 27005

Toda empresa pública o privada, formal o informal se crea y mantiene con miras a alcanzar la visión y objetivos determinados.

La variedad de los posibles eventos que pueden afectar de forma negativa el cumplimiento de los objetivos establecidos pueden considerarse infinitos. Estos eventos pueden tener origen interno o externo, pueden ser intencionados o no y tener naturaleza de diferente índole, tales como: riesgos financieros, operativos, tecnológicos, de mercado, legal, de seguridad de la información, etc.

El análisis de riesgos es una herramienta que permite identificar, clasificar, y valorar los eventos que pueden amenazar la consecución de los objetivos de la organización y establecer las medidas oportunas para reducir el impacto esperable hasta un nivel tolerable.

Dentro del análisis de riesgos de la seguridad de la información se pueden tener diferentes responsables dentro de la organización, algunos de estos responsables puedes ser:

Responsables de seguridad de la información, el cual define el plan de acción necesario para cumplir los requerimientos de la organización.

Dirección de la organización, debido a la necesidad de establecer medidas contra los riesgos que amenazan la consecución de los objetivos fijados.

Los Auditores, debido a que necesitan obtener y mantener un profundo conocimiento de los riesgos existentes de la organización, que empleen su función de evaluar el cumplimiento de las políticas y procedimientos establecidos para mitigarlos.

Estándar para la gestión de riesgos de seguridad

a) **Contexto fase de establecimiento:** Esta fase se definen todos los objetivos así como el alcance y la organización de todo el proceso dando inicio una vez que se tiene toda la información acerca del caso que se desea evaluar, para lograr bien esto se necesita el establecimiento de criterios como lo son:
   - Criterios de evaluación de riesgos.
   - Criterios de impacto.
   - Criterios de aceptación del riesgo

Entre otros, luego se deben definir tanta el alcance como los límites de todos los activos relevantes, los objetivos de negocio, procesos de negocio, estrategias y políticas, legales y los requisitos reglamentarios aplicables a la organización, interfaces, etc. y el establecimiento de una organización apropiada de utilizar la seguridad de la información de gestión de riesgos como las funciones y responsabilidades.

Esta fase de divide en dos las cuales son contexto interno y contexto externo de la siguiente manera:

Contexto interno: entonces es necesario el conocer la organización internamente como su estructura interna, el personal, recursos humanos, filosofía y valores, políticas, misión, metas, objetivos y estrategias para lograrlos.

- Fase de Identificación de Riesgos.
- Estimación del riesgo.
- Riesgo de la fase de evaluación.

Aunque muchos motivos de índole de seguridad y de protección se conviertan en el motor que sostiene proyectos, es evidente que surge un problema con la privacidad personal y empresarial que se está convirtiendo en una ilusión difícil de alcanzar.

Cada vez es más evidente la necesidad de compartir información con más rapidez y facilidad, y el internet ha sido la respuesta clara. Pero también se plantean retos sobre el límite de la seguridad que posee esta cuando se intercambia y parece ser que cada vez es más difícil mantener incluso secretos de índole político y económico.

CAPÍTULO IV
AUDITORÍA INTERNA GUBERNAMENTAL INFORMÁTICA, EVALUACIÓN DEL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN, DE UNA ENTIDAD AUTÓNOMA Y DESCENTRALIZADA
(CASO PRÁCTICO)

4.1 Antecedentes

El Instituto Autónomo y Descentralizado de Salud creado 30 de octubre de 1946 inicia como una consecuencia de la segunda guerra mundial y la difusión de ideas democráticas en el mundo, el 20 de octubre de 1944 se derrocó al gobierno del General Federico Ponce Vaides y se eligió un gobierno democrático, bajo la presidencia del Doctor Juan José Arévalo. El Gobierno de Guatemala de aquella época, gestionó la venida al país de dos técnicos en materia de Salud, quienes hicieron un estudio de las condiciones económicas, geográficas, étnicas y culturales de Guatemala. Al promulgarse la Constitución de la República de aquel entonces, el pueblo de Guatemala, encontró entre las Garantías Sociales, "UN RÉGIMEN NACIONAL, UNITARIO Y OBLIGATORIO DE SALUD, DE CONFORMIDAD CON EL SISTEMA DE PROTECCIÓN MÍNIMA". La Ley regulaba sus alcances, extensión y la forma en que debía ser puesto en vigor. El 30 de octubre de 1946, el Congreso de la República de Guatemala, emite el Decreto número 296. Creando así "Una Institución autónoma, de derecho público de personería jurídica propia y plena capacidad para adquirir derechos y contraer obligaciones, cuya finalidad es aplicar en beneficio del pueblo de Guatemala, un régimen nacional, unitario y obligatorio de salud, de conformidad con el sistema de protección mínima". Un régimen nacional, unitario y obligatorio, esto significa que debe cubrir todo el territorio de la República, debía ser único para evitar la duplicación de esfuerzos y de cargas tributarias, sin evadir sus obligaciones, pues ello significaría incurrir en la falta de salud.

4.1.1 Generalidades

El Instituto Autónomo y Descentralizado de Salud inicia con sus actividades el 30 de octubre de 1946 con alrededor de 1,500 empleados los que en la actualidad se incrementaron, hasta llegar a contar con alrededor de 12,000 empleados, la atención a sus pacientes se refleja en una afluencia 1,500 personas por día. Mejorando los procesos con la implantación de nuevas tecnologías que permitan contar con una adecuada gestión para que estos simplifiquen el trabajo, agilizando procesos de atención, hasta alcanzar la satisfacción de los pacientes.

El Gerente del Instituto por medio del Acuerdo No. 1840 de fecha 21 de diciembre de 1973, cambió la denominación del Departamento de Tabulación y Registros Mecanizados a la de Departamento de Procesamiento Electrónico de Datos; sin embargo con el Acuerdo número 1048 de Junta Directiva de fecha 12 de marzo de 1998, crea la Dirección General de Informática, la que dentro de sus funciones fue la de proponer las políticas que permitan un adecuado desarrollo de sistemas de información, para brindar en este sentido el apoyo necesario para la modernización del Instituto en las distintas áreas de trabajo. El Departamento de Procesamiento Electrónico de Datos pasó a depender de la Dirección antes mencionada.

Con el Acuerdo número 1164 de Junta Directiva de fecha 11 de agosto de 2005, quedó suprimida la Dirección General de Informática, y se modificó la denominación del Departamento de Procesamiento Electrónico de Datos a Departamento de Informática, dependiendo este último de la Subgerencia de Planificación y Desarrollo. Pero el Acuerdo número 1199 de Junta Directiva de fecha 02 de noviembre de 2006, se suprime de la línea jerárquica de la Subgerencia de Planificación y Desarrollo al Departamento de Informática pasando este por adición a la Subgerencia Administrativa.

En la actualidad la Junta Directiva del Instituto desea que se implemente un conjunto de procedimientos, estructuras y comportamientos que servirán para dirigir y controlar la organización hacía el logro de sus objetivos, por lo que se hace necesario contar con un gobierno de tecnologías de la información que

provea las estructuras que unan los procesos de TI, los recursos de TI y la información con las estrategias y los objetivos de la institución, con buenas (o mejores) prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoriza el rendimiento de TI, para asegurar que la información de la institución y las tecnologías, relacionadas soportan sus objetivos del negocio. El gobierno de tecnologías de la información, conducirá a la institución a tomar total ventaja de su información logrando maximizar sus beneficios a la población Guatemalteca.

Nombramiento No. 1-1-2016

4.2 Nombramiento

Guatemala, 01 de febrero de 2016

Auditor Interno:
Christian David Sumale Chocoj

De conformidad con el Plan Anual de Auditoría para el ejercicio 2016, se le designa para que se constituya en el Departamento de Informática del Instituto Autónomo y Descentralizado de Salud, para que practique una evaluación en el área de Gobierno de Tecnologías de Información.

El origen de esta evaluación está contenido en el Plan Anual de Auditoría del Ejercicio 2016.

El objetivo de la evaluación es:

Evaluar las buenas prácticas de Gobierno de Tecnologías de la Información para la institución

Alcance

1. La alineación estratégica del Gobierno de Tecnologías de la Información.
2. Políticas, estándares y procedimientos de TI.
3. La continuidad de servicio de las Tecnologías de la Información.
4. Gestión sobre el RRHH y las directrices de Gobierno emitidas para el efecto.
5. Directrices de Gobierno sobre la gestión de infraestructuras y aplicaciones de Tecnologías de Información.
6. Decisiones de alto nivel que permitan contar con una seguridad razonable en la protección y disponibilidad de datos.

El período a revisar será del 1 de enero al 31 diciembre 2015.

El plazo que se les asigna para llevar a cabo la auditoría será del **01 al 19 de febrero de 2016** (incluye planificación específica y trabajo de campo) y la fecha establecida para la entrega del informe es el **29 de febrero de 2016**, el cual se deberá presentar en cumplimiento a los lineamientos establecidos en el Departamento de Auditoría Interna.

Derivado de la evaluación deberá entregar un informe con su opinión global sobre la práctica de Gobierno de Tecnologías de Información y áreas de mejora que se pudieran presentar.

Atentamente,

Licenciado Erwin José Ericastilla López
Jefe del Departamento de Auditoría Interna

4.3 Planificación del trabajo

Comprenderá el desarrollo de una estrategia global para establecer un enfoque apropiado sobre la naturaleza, oportunidad y alcance de los procedimientos de auditoría que deberán aplicarse. El planeamiento también permitirá hacer uso apropiado del potencial humano disponible.

4.3.1 Entorno de Control

La Gestión de tecnologías de la información está a cargo del Jefe del Departamento de Informática, el cual gestiona las TI, pero no es quien toma las decisiones, se encuentra el Departamento de Informática bajo la línea jerárquica de la Subgerencia Administrativa, quien es el responsable de reportar a la máxima autoridad los cambios y propuestas para la adecuada gestión de las TI.

La Gestión de las tecnologías de la información se realiza basándose en las normas de la familia ISO 27000, específicamente toma en cuenta las normas ISO 27001, 27002 y 27005; asimismo, se apoya en el marco de referencia COBIT, con estos marcos de referencia, normas y buenas prácticas se delimitan las directrices de TI.

El Departamento de Informática cuenta con manuales, mismos en los que se plasman las directrices que a consideración de este departamento, ayudaría a la adecuada gestión de las TI.

Los sistemas informáticos no son compatibles según el formato en el que se almacena dicha información la gran mayoría son aplicaciones web modernas, desarrolladas en un ambiente .NET y HTML, pero existen sistemas auxiliares a estos como el sistema AS/400, que es un tanto obsoleto, y que no es compatible para la migración de datos. En cuanto a la topología de red, se considera una topología híbrida, con una categoría 6 de cableado estructurado de red, el centro de datos se encuentra ubicado en el tercer nivel de las oficinas centrales de la institución, el mismo cuenta con medidas de seguridad como lo son extintores de incendios, detectores de humo y alarma de siniestros.

4.4 Áreas Críticas y Evaluación de Factores de Riesgo

Derivado del proceso de la familiarización, se detectaron áreas críticas, que se conviertan en factores de riesgo que presenten eventualmente algunas limitaciones, que impidan obtener un grado razonable de confiabilidad sobre la dirección, control, registro, información, cumplimiento de aspectos legales, técnicos, etc., para ejecutar la auditoría, por lo que serán objeto de análisis más extensivo en la ejecución del trabajo de auditoría siendo los siguientes:

4.4.1 Riesgo inherente:

- Que el personal presente resistencia a las TI.
- Que las directrices no sean comprendidas.
- Que las capacidades del personal que esté involucrado en el gobierno de tecnologías de la información no posea las capacidades técnicas ni los conocimientos necesarios para la implementación de este.
- Que los activos tecnológicos sean obsoletos.
- Que la alta gerencia no emita directrices correctas de TI.

4.4.2 Riesgo de control:

- Manuales no actualizados.
- Directrices a nivel de Junta Directiva, pero no convertidas.
- Emisión de directrices de TI, no contemplan todo el alcance de la gestión.
- Inadecuada segregación de funciones.

4.4.3 Tipos de pruebas

Las técnicas de auditoría que servirán para realizar las pruebas para obtener evidencia necesaria que fundamente su opinión. Se detallan a continuación:

- Observación
- Cuestionario
- Entrevista
- Elaboración de matrices

- Revisión documental
- Confirmación
- Análisis de procesos
- Comparaciones
- Corroboración de información oral contra documental

4.5 Alcance

El alcance del trabajo a realizar será la evaluación de la Gestión del Gobierno de Tecnologías de la Información, basado en la alineación estratégica; políticas, estándares y procedimientos; la continuidad de los servicio de las Tecnologías de la Información; gestión sobre el recurso humano y las directrices de Gobierno emitidas para el efecto; así como, la gestión de infraestructuras y aplicaciones de Tecnologías de Información y las decisiones de alto nivel que permitan contar con una seguridad razonable en la protección y disponibilidad de datos, que comprende el periodo del 01 de enero al 31 de diciembre 2015.

4.6 Recursos

a) Recurso Humano

1 Supervisor de Auditoría

1 Asistente de Auditoría

b) Recursos Financieros

Salarios de personal asignado por 21 días de duración de la revisión:

Asistente de Auditoría de Informática con un estimado de Q.4,550.00

Jefe de Departamento de Auditoría Interna con un estimado de Q.11,900.00

c) Recursos Físicos

1 Computadora tipo laptop con acceso al grupo de dominio de red Institucional.

d) Sistemas Informáticos

- Acceso a los sistemas:
- Software informático de escaneo de equipos
- Spark
- Correo institucional
- AS-400
- SICOIN-WEB
- SIIADS
- Privilegios de acceso especial de administrador de la red de dominio IADSGT.ORG.

4.7 Criterios de Selección de Muestras

Se utiliza la técnica de muestro sobre atribuciones, basado en la importancia de:

- Personal clave de procesos de gestión.
- Documentos y directrices del Gobierno de TI.
- Procesos que apoyan directamente la gestión de TI.

4.8 Cronograma

No.	ACTIVIDADES	MES DE FEBRERO 2016														
		1	2	3	4	5	8	9	10	11	12	15	16	17	18	19
1	**Planificación**															
5	**Ejecución del trabajo de campo**															
	Comunicación de resultados															

Instituto Autónomo y Descentralizado de Salud

Cuestionario de Evaluación del Gobierno de Tecnologías de la Información

Periodo de Evaluación del 01 de enero al 31 de diciembre de 2015

Objetivo:

Obtener información primaria sobre el gobierno de tecnologías de información en la institución.

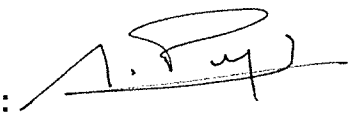
Dirigido a: Jefe del Departamento de informática

No.	Pregunta / Descripción	SI	NO	Comentario
1	¿Existen directrices específicas para el departamento de informática?	✓		Se tiene conocimiento, sin embargo, no se han dado a conocer a todas las líneas interesadas.
2	¿Se poseen planes determinados que impulsen estrategias de informática?		✓	La prioridad va enfocada a otros departamentos de la institución.
3	¿El departamento de informática posee un marco de referencia para realizar sus actividades?	✓		Su marco de referencia es las Normas ISO 27000.
4	¿Existe algún comité involucrado en la tecnología de información de la institución?		✓	No se ha contemplado la creación de algún comité.
5	¿Existen políticas y procedimientos establecidos para los procesos que realizan los encargados del departamento?	✓		Existen pero no todos tienen conocimiento de ello.
6	¿Los procesos de tecnología de información se dan a conocer al elemento humano?	✓		Se dan a conocer como parte de la inducción y no de manera escrita.
7	¿Al realizar un proyecto de informática se analiza la viabilidad del mismo?	✓		Si, se determina según la necesidad de la institución.

Elaborado por: Christian David Sumale Chocoj, **Auditor interno.**

Responsable de responder: Diego Antonio Pérez Méndez, **Jefe del Departamento de Informática**

Firma: 

Firma: 

Instituto Autónomo y Descentralizado de Salud

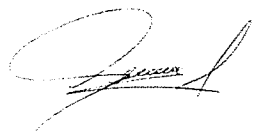
Cuestionario de Evaluación del Gobierno de Tecnologías de la Información

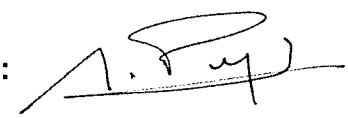
Periodo de Evaluación del 01 de enero al 31 de diciembre de 2015

No.	Pregunta / Descripción	SI	NO	Comentario
8	¿Existen estándares definidos de adquisición de activos o servicios tecnológicos en la institución?	✓		Si se definen al iniciar las adquisiciones con un estándar propuesto por el Departamento de Informática.
9	¿En la adquisición de activos o servicios tecnológicos, se involucra una persona experta que asesore el proceso?	✓		Se adquiere el servicio de un experto a través del tipo de adquisición.
10	¿Los activos tecnológicos poseen políticas sobre el valor depreciable y valuaciones con tiempo definido?	✓		Están establecidas y las valuaciones no tienen un tiempo definido.
11	¿Al implantar algún sistema se analiza respecto a las capacidades del personal para que el aprovechamiento del recurso sea óptimo?		✓	No se toman en cuenta las capacidades del personal.
12	¿Los sistemas brindan información oportuna?	✓		Si, debido a que cuentan con calidad en los procesos.
13	¿Las personas encargadas a informática se han capacitado para el manejo de nuevas tecnologías dentro de la institución?	✓		Se han capacitado al personal según el avance tecnológico adoptado.
14	¿Las personas se han resistido al cambio en función a utilización de equipos tecnológicos y sistemas automatizados?	✓		Existen algunos casos que se han resistido a realizar sus labores han cometido errores.

Elaborado por: Christian David Sumale Chocoj, **Auditor interno.**

Responsable de responder: Diego Antonio Pérez Méndez, **Jefe del Departamento de Informática**

Firma: 

Firma: 

Instituto Autónomo y Descentralizado de Salud

Cuestionario de Evaluación del Gobierno de Tecnologías de la Información

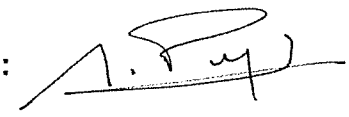
Periodo de Evaluación del 01 de enero al 31 de diciembre de 2015

No.	Pregunta / Descripción	SI	NO	Comentario
15	¿Se evalúan el desempeño en el área de informática?		✓	De manera general a todos los empleados.
16	¿Se han detectado deficiencias en los resultados respecto al desempeño sobre la tecnología de información?	✓		En algunas ocasiones por errores operacionales.
17	¿Existe un compromiso institucional donde se le da la importancia que representa la tecnología de información?		✓	No es reflejado de manera escrita.
18	¿Se conocen propuestas para definir al departamento de Informática a una línea jerárquica más alta?		✓	No se tiene contemplado desligar el Departamento de Informática de la Subgerencia Administrativa.
19	¿Se tiene contemplado realizar modificaciones a perfiles de puestos acorde a los objetivos de informática?		✓	No debido a que esta actividad es exclusiva de la Junta Directiva de la Institución.
20	¿Se posee un plan de mejora continua en el equipo informático en los próximos años?	✓		Se posee dicho plan pero no está definido el periodo.

Elaborado por: Christian David Sumale Chocoj, **Auditor interno.**

Responsable de responder: Ing. Diego Antonio Pérez Méndez, **Jefe del Departamento de Informática**

Firma: 

Firma: 

4.9 Ejecución del Trabajo

Programa de Trabajo

Entidad: Instituto Autónomo y Descentralizado de Salud

Tipo de Auditoría: Auditoría informática

Área: Evaluación del Gobierno de Tecnologías de la Información

Periodo a Examinar: Del 01 de enero al 31 de diciembre de 2015

No.	Descripción	Referencia	Elaboró	Fecha
1.	**Definición**			
	El gobierno de tecnologías de la información provee las estructuras que unen los procesos de tecnologías de la información, los recursos de tecnologías de la información y la información con las estrategias y los objetivos de la empresa; además, el gobierno de tecnologías de la información integra e institucionaliza buenas (o mejores) prácticas de planificación y organización; adquisición e implementación; entrega de servicios y soporte; y, monitoriza el rendimiento de TI para asegurar que la información de la empresa y las tecnologías relacionadas soportan sus objetivos del negocio.			
2	**Objetivo**			
	Obtener evidencia para emitir juicios y una opinión global, acerca de si existe un gobierno de tecnologías de la información, mediante la definición de metodologías y procesos de Auditoría Interna que permitan alcanzar los objetivos del Departamento de Auditoría Interna.			

No.	Descripción	Referencia	Elaboró	Fecha
3	**Alcance**			
	La evaluación de la Gestión del Gobierno de Tecnologías de la Información, basado en la alineación estratégica; políticas, estándares y procedimientos la continuidad de los servicio de las Tecnologías de la Información; gestión sobre el recurso humano y las directrices de Gobierno emitidas para el efecto, la gestión de infraestructuras y aplicaciones de Tecnologías de Información; así como, las decisiones de alto nivel que permitan contar con una seguridad razonable en la protección y disponibilidad de datos, que comprende el periodo del 01 de enero al 31 de diciembre 2015.			
4	**Trabajo a Desarrollar**			
	Entreviste a funcionarios y personal clave para obtener información sobre el grado de conocimiento del Gobierno de Tecnología de la Información actual en la Institución a) Secretario de Junta Directiva b) Subgerente Administrativo c) Subgerente Financiero d) Subgerente de Recursos Humanos e) Subgerente de Planificación y Desarrollo f) Jefe de Informática	**A**	**CS**	**08/02/2016**

No.	Descripción	Referencia	Elaboró	Fecha
	Solicite a la Junta Directiva el Plan Estratégico Institucional que comprende al periodo de 01 de enero al 31 de diciembre del 2015 y obtenga información sobre los siguientes aspectos: • Alineación de Estrategias institucionales y el área de Informática en donde se establezca la interrelación entre los objetivos de TI y los principios de Gobierno de TI, propuesto por la Norma ISO 38500.	**B**	**CS**	**08/02/2016**
	Solicite a la Gerencia Administrativa el Acuerdo de funcionalidad del departamento y verifique si cumple con los principios de Gobierno de Tecnología de la Información, contenidos en la Norma ISO 38500.	**C**	**CS**	**08/02/2016**
	Entreviste al Jefe de Informática sobre iniciativas de implantación de nuevas plataformas informáticas y si posee experiencia y conocimiento sobre el manejo de dicho sistemas; así como, la capacidad Instalada es adecuada para la implantación de un nuevo sistema para garantizar la continuidad de servicio de las Tecnologías de la Información.	**D**	**CS**	**15/02/2016**
	Entreviste al Jefe de Informática y al Gerente de Recursos humanos a efecto de confirmar lo siguiente: a. Existen perfiles definidos para la selección de los colaboradores a contratar. b. El personal que lleva a cabo las actividades del departamento de informática se encuentra debidamente capacitado para desempeñar sus funciones.	**E**	**CS**	**15/02/2016**

No.	Descripción	Referencia	Elaboró	Fecha
	Verifique en el Departamento de Informática sobre directrices de Gobierno de la gestión de infraestructuras y aplicaciones de Tecnologías de Información.	F	CS	15/02/2016
	Realice una matriz sobre el nivel de madurez para determinar si las decisiones de alto nivel permitan contar con una seguridad razonable en la protección y disponibilidad de datos por cada uno de los principios de la Norma ISO 38500 que a continuación se detallan: a. Responsabilidad b. Estrategia c. Cumplimiento d. Comportamiento de recurso humano e. Adquisición f. Desempeño	G	CS	15/02/2016
5	Cruce la información y referenciación necesaria.			
6	Elabore el informe correspondiente.			

Elaborado por:

Christian David Sumale Chocoj, Auditor Interno

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 12 de febrero de 2016

Firma

Instituto Autónomo y Descentralizado de Salud

Periodo de 01 de enero al 31 de diciembre de 2015

Sumaria de la Evaluación de Gobierno de TI actual en la Institución

Ref. P/T	Descripción	Grado de Conocimiento de la Administración del Gobierno de TI ⬟
A1	**Entreviste al personal clave:**	
1	Secretario de Junta Directiva	**Medio**
2	Subgerente Administrativo	**Medio**
3	Subgerente Financiero	**Medio**
4	Subgerente de Recursos Humanos	**Medio**
5	Subgerente de Planificación y Desarrollo	**Medio**
6	Jefe de Informática	**Alto**

Conclusiones:

- Se determinó al analizar el comentario del personal clave que existe falta de comunicación entre este personal debido a que la Junta Directiva tiene contemplado proyectos que no han sido comunicados al ente rector de los procedimientos informáticos que en este caso al Departamento de Informática.
- Se determinó que la estructura organizacional y operacional del Departamento de Informática no es el adecuado debido a que depende de la Subgerencia Administrativa, y no existe independencia ni un criterio objetivo en la toma de decisiones.
- Se determinó que dentro de la máxima autoridad de la institución no se ha contemplado una comisión designada para supervisar la gestión y administración de los activos tecnológicos.

Por lo anterior se emitirá una observación por el área de mejora.

⬟ Ver criterios de Grado de Conocimiento en **Cédula de Criterio de Grado de Conocimiento**.

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula narrativa de procedimientos del Gobierno de TI actual en la Institución

Objetivo:

Obtener evidencia si la Junta Directiva del Instituto tiene conocimientos o ha establecido una estructura de gobierno de tecnologías de la información y si el mismo es adecuado.

Alcance:

La evaluación de la Gestión del Gobierno de Tecnologías de la Información, basado en la alineación estratégica; políticas, estándares y procedimientos.

Persona a Entrevistar: Secretario de Junta Directiva

Como parte de las funciones de la Honorable Junta Directiva se conocen únicamente las propuestas que realiza el Departamento de Informática o de su autoridad la Subgerencia Administrativa, realmente no se tiene a una comisión encargada de que vea el tema de tecnologías que evalué si estas son adecuadas para el instituto, o si las existentes son las en realidad necesita la institución, en este caso el señor Gerente propone y se toman las decisiones con base a lo que el análisis de gerencia dictamina, de igual forma no se toma la decisión de todas las adquisiciones debido a que la Ley de Contrataciones del Estado delimita quien debe tomar decisiones y si esta le corresponda a la Junta Directiva; así mismo, desde el año 2015 se estimó la adquisición de una nueva plataforma informática que permita mejorar la administración tanto de los recursos financieros como la administración de los expedientes médicos para lo cual se tiene contemplado adquirir el plataforma denominada "Sistemas, Aplicaciones y Procesos (SAP).

F. **F.**

Persona Encuestada **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud
Evaluación de Gobierno de TI
Entrevistas a Personal Clave
Periodo de 01 de enero al 31 de diciembre de 2015

Persona a Entrevistar: Subgerente Administrativo

Conozco del Gobierno de Tecnologías de la Información, y que el mismo es importante para el mejor aprovechamiento de los recursos tecnológicos pero que debido a solicitudes de Gerencia se prioriza en mantener políticas de austeridad para maximizar y eficientar los recursos económicos esa es la razón por la cual se hace algo complejo el realizar el implementar una adecuada estructura que gestione de una manera adecuada al Gobierno de Tecnologías de la Información; asimismo, la Honorable Junta Directiva ha solicitado se conforme una comisión que permita establecer mejores políticas para aprovechar los activos tecnológicos de una mejor manera. Dentro de los mismos planes de Junta Directiva se plantea la adquisición de una nueva plataforma que permita administrar de una mejor forma los recursos financieros y que mejore los procesos, evitando así el excesivo papeleo y la agilización del otorgamiento de servicios por parte de esta institución.

F. _____
Persona Encuestada

F. _____
Auditor Interno

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Entrevistas a Personal Clave

Periodo de 01 de enero al 31 de diciembre de 2015

Persona a Entrevistar: Subgerente Financiero

Mi función específica es proponer políticas para la correcta administración de los recursos por lo que en cuanto a la participación de esta Subgerencia en el Gobierno de Tecnologías de la Información, creo que debe delimitarse a poner a disposición de Junta Directiva, Subgerencia Administrativa y Departamento de informática, análisis de impacto en cuanto a la adquisición de nueva tecnología o la implementación de políticas si estas últimas representan erogaciones, con el objetivo de no descuidar la parte de manejar los fondos institucionales con efectividad, eficiencia y economía.

F. **Persona Encuestada**

F. **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Entrevistas a Personal Clave

Periodo de 01 de enero al 31 de diciembre de 2015

Persona a Entrevistar: Subgerente de Recursos Humanos

Se tiene conocimiento de la importancia del Gobierno de Tecnologías de la Información, la subgerencia de recursos humanos tiene a su cargo funciones importante dentro del Gobierno de TI, debido a que somos quien dotamos de personal al Departamento de informática, pero en la mayoría de ocasiones se hace imposible poder contratar personal calificado que es experto en el tema, debido a que se pretende tener una política de austeridad y no se aprueban nuevas plazas con personal calificado y únicamente se trabaja con el personal que ya labora, como salida a la falta de personal antes descrita la Subgerencia Administrativa, quien es la unidad ejecutora del Departamento de informática, contrata personal en el renglón 029 "Otras remuneraciones de personal temporal", para suplir la falta de personal calificado.

F. **Persona Encuestada**

F. **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Entrevistas a Personal Clave

Periodo de 01 de enero al 31 de diciembre de 2015

Persona a Entrevistar: Subgerente de Planificación y Desarrollo

Se tienen propuestas para mejorar la organización de la institución, sin embargo es algo que se realiza paulatinamente y no es de forma inmediata por lo que si la Junta Directiva lo estima conveniente el podrá realizar una propuesta para poder implementar una adecuada estructura que sea acorde a las nuevas tendencias a nivel internacional en cuanto al manejo de los sistemas de información.

F. **Persona Encuestada**

F. **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Entrevistas a Personal Clave

Periodo de 01 de enero al 31 de diciembre de 2015

Persona a Entrevistar: Jefe del Departamento de Informática

Explico que dentro de sus aportes a la institución se encuentra el proyecto de implementar una mejor estructura de Gobierno de Tecnologías de la información; aunque se ha obtenido el apoyo de las autoridades de la institución el proceso es un poco lento debido a que se necesita actualizar procedimientos y normativas; así mismo, no se tiene conocimiento si se desea implementar nuevas plataformas, y la incertidumbre es debido a que el instituto cuenta con alrededor de 60 aplicaciones que no interactúan entre sí por lo que la gestión se hace ineficiente y sería excelente poder tener una nueva plataforma que concentrara de una mejor forma la información y que pueda ser gestionada de una mejor manera.

Comentario:

El Plan Estratégico de la institución del periodo comprendido como parte del cumplimiento del mismo involucra a distintos niveles de la institución que deben promover las mejoras prácticas de gobierno de TI, en cada una de las funciones relacionadas. El gobierno de TI posee estructuras, aplicaciones, operaciones y sistemas que son ejecutas por recurso humano que cumplan con un perfil establecido que a conocimiento de estrategias se desempeñan a través de lineamientos, reportes y requerimientos de resultados acorde al cumplimiento de los objetivos definidos. De tal manera que los involucrados en la actividad de informática deben conocer sus funciones y el aporte que le brindan al Departamento.

F. **Persona Encuestada**

F. **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud
Periodo de 01 de enero al 31 de diciembre de 2015
Sumaria de la Evaluación de la Alineación del Gobierno de TI

Ref. P/T	Descripción	Nivel de Alineación*	Interrelación entre los Objetivos de TI y el modelo de Gobierno Propuesto por la ISO 38500**
B-1	Alineación de Estrategias institucionales y el área de Informática en donde se establezca la interrelación entre los objetivos institucionales y los principios de Gobierno de TI.	Bajo	
			Inicial

Conclusiones:

a) Se determinó al analizar los objetivos estratégicos institucionales y los objetivos de TI, que estos carece de una de las tareas principales del Gobierno de TI, "Aprendizaje y Crecimiento" para poder implantar un adecuado gobierno de tecnologías de la información, debido a que la institución actualizo sus objetivos estratégicos, sin actualizar los objetivos de TI, por lo que se denota una falta alineación, planificación y organización para poder establecer un adecuado Gobierno de TI.

b) Al comparar los objetivos de TI de la Institución con el modelo de gobierno propuesto por la Norma ISO 38500, basado en los principios seis principios de Gobierno de TI, la institución contempla únicamente ocho de estas propuestas para garantiza la adecuada gestión de TI.

Por lo anterior se emitirá una observación por el área de mejora.

*** Nivel de Alineación:**

Bajo: La alineación entre los objetivos Institucionales y los del área de TI, carecen de una alineación objetiva que se interrelacionen.
Medio: Existe alineación entre algunos objetivos institucionales y los objetivos de TI.
Alto: Los objetivos institucionales y los objetivos de TI, estan alineados adecuadamente.

****Interrelación entre los Objetivos de TI y el modelo de Gobierno Propuesto por la ISO 38500**

Inicial: Los objetivos de TI, no se cubren todos los principios de la Norma ISO 38500.
Intermedio: Los objetivos de TI, cubren algunos principios de la Norma ISO 38500.
Avanzado: Los objetivos de TI, cubren todos los principios de la Norma ISO 38500.

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula narrativa de procedimientos de correlación entre el Plan Estratégico Institucional y los objetivos de TI actuales en la Institución

Objetivo:

Obtener evidencia si los objetivos estratégicos institucionales y los objetivos de tecnologías de la información presentan una correlación adecuada.

Alcance:

La evaluación de la Gestión del Gobierno de Tecnologías de la Información, basado en la alineación estratégica; políticas, estándares y procedimientos.

Trabajo realizado:

Se solicitó a la Junta Directiva del Instituto, que trasladara al auditor actuante fotocopia de los objetivos estratégicos institucionales; así mismo, se solicitó al Jefe del Departamento de Informática al auditor copia de los objetivos de TI, para su respectiva comparación para lo cual se tomara como referencia COBIT 5, para establecer si dichos objetivos están alineados de manera adecuada.

Se realizó un estudio con el Jefe del Departamento de Informática, conforme a la "Cascada de Metas" para traducir las necesidades de las partes interesadas en metas corporativas y metas relacionadas con las TI, útiles y a medida. Esto permite establecer metas específicas en todos los niveles y en todas las áreas de la institución en apoyo de los objetivos generales y requisitos de las partes interesadas y así, efectivamente, soportar la alineación entre las necesidades de la empresa y las soluciones y servicios de TI, se indago y pudo determinarse que los objetivos de TI, están desactualizados debido a que fueron modificados los objetivos estratégicos de la Institución a continuación se detallan los pasos de análisis de alineación:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula narrativa de procedimientos de correlación entre el Plan Estratégico Institucional y los objetivos de TI actuales en la Institución

- Paso 1. Establecer si las partes interesadas influyen en las necesidades de la Institución.
- Paso 2. Las necesidades de las partes interesadas desencadenan en objetivos Institucionales.
- Paso 3. La cascada de Metas de la Institución está relacionada con las de TI.
- Paso 4. Para determinar la priorización de los objetivos se establece la correlación entre el objetivo institucional y el de TI, como Principal "P" y Secundario "S", lo que determinara cuan alineados están dichos objetivos y si con los mismos se puede establecer una adecuada estructura de Gobierno de Tecnologías de la Información.

Los pasos realizados y análisis se compilaron en una matriz de alineación. Ver en **B-1.5/7**

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

PLAN ESTRATEGICO GENERAL

CFO

El Plan Estratégico de la institución para el periodo comprendido del año 2013-2017, permitirá adoptar líneas de acción específicas y de evaluación de resultados sobre la base de las vertientes de trabajo establecidas en el mismo, y que le dan continuidad a lo esencial del Plan Estratégico 2008-2012.

Con este plan se establecen metas concretas para proporcionar un mejor servicio a los derechohabientes, mejorar la integridad de los programas institucionales, avanzar en la modernización tecnológica y fortalecer la planeación y administración de los seguros.

El plan busca dar un mensaje claro de que, si bien se requiere una solución a los problemas estructurales, en un horizonte perceptible por todos, es posible llevar a cabo inversiones en tecnología, capacitación al personal, análisis de política social y financiera, renovación de procesos y fortalecimiento del control, de manera que el Instituto se prepare para resolver las necesidades futuras de los derechohabientes.

Un elemento que por su importancia y relevancia se convierte en uno de los principales retos a superar, lo constituye la institucionalización de los sistemas de información diseñados, desarrollados e implantados en los últimos años, mismo que, al igual que todo sistema, requiere de la evaluación y diagnóstico continuo.

Bajo esta perspectiva, las prioridades se agrupan en:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Plan Estratégico Institucional

Periodo de 01 de enero al 31 de diciembre de 2015

- Ampliación de cobertura.
- Solidez financiera.
- Prestaciones de calidad.
- Eficiencia, transparencia y control.
- Crecimiento y desarrollo institucional.
- Transparentar los procesos de contrataciones en general.
- Automatizar a l Instituto Autónomo y Descentralizado de Salud.
- Continuar con las acciones para evitar la corrupción.
- Dignificar a los trabajadores por medio de la meritocracia y propiciar la Carrera Administrativa.
- Capacitar en servicio al personal del IADS para mejorar la atención de los usuarios.
- Agilizar los proyectos de infraestructura que están en proceso de ejecución.

Orden	Objetivo TI
1	Planificar, coordinar y supervisar funciones y actividades asignadas a las, Divisiones de Desarrollo de Sistemas y de Operaciones que tiene bajo su cargo.
2	Analizar, diseñar, desarrollar y supervisar sistemas informáticos que apoyan los procesos de las dependencias del Instituto.
3	Formular proyectos de tecnología y gestionar la adquisición del equipo informático para implementarlos.
4	Instalar y supervisar el funcionamiento de los nuevos sistemas informáticos.
5	Asesorar y coordinar las actividades informáticas que se desarrollan en las dependencias del Instituto.
6	Capacitar y facilitar soporte técnico a usuarios de los sistemas informáticos.
7	Implementar y supervisar el funcionamiento de sistemas de telecomunicación y nuevas plataformas tecnológicas.
8	Proponer, implementar y cumplir normas de seguridad para el funcionamiento, uso y manejo de los sistemas y equipo informático, a nivel institucional.

Instituto Autónomo y Descentralizado de Salud

Evaluación del Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Relación entre Objetivos TI y Objetivos de la Institución

		Objetivos TI	Objetivos Estratégicos de la Institución										
			Continuar con el desarrollo e implementación de la reingeniería de procesos e incorporación de tecnología	Incorporar tecnología a los procesos de trabajo de los servicios contratados.	Incorporar tecnología para el control y modernización de los procesos de trabajo.	Adquirir equipo para fortalecer las redes (conectividad o enlace de fibra óptica y otros)	Adquirir equipo para fortalecer la capacidad de almacenamiento del Data Center.	Diseñar, rediseñar, desarrollar e implementar herramientas informáticas y aplicación de la mejora	Integrar e institucionalizar las herramientas informáticas.	Aprovechar la transferencia de conocimiento y tecnología con organismos especializados en salud.	Elaborar propuesta de implementación de firma electrónica en la solicitud de pedido electrónico SA-6 (proyecto piloto)	Implementar el expediente médico electrónico, incluyendo firma electrónica
			1	2	3	4	5	6	7	8	9	10
			Financiera					Interna		Cliente		
Evaluar, Orientar y Supervisar	1	Planificar, coordinar y supervisar funciones y actividades asignadas a las, Divisiones de Desarrollo de Sistemas y de Operaciones que tiene bajo su cargo.	P	S	S		S	P	P	S	P	S
	2	Analizar, diseñar, desarrollar y supervisar sistemas informáticos que apoyan los procesos de las dependencias del Instituto.	P	P	P	S	P	P	S	P	S	S
	3	Formular proyectos de tecnología y gestionar la adquisición del equipo informático para implementarlos.	S	P	P		P	P	S	P	P	P
	4	Instalar y supervisar el funcionamiento de los nuevos sistemas informáticos.	P	P	P		P	P		P	S	S
	5	Asesorar y coordinar las actividades informáticas que se desarrollan en las dependencias del Instituto.	S			S	S	S		S	P	P
	6	Capacitar y facilitar soporte técnico a usuarios de los sistemas informáticos.							P			
	7	Implementar y supervisar el funcionamiento de sistemas de telecomunicación y nuevas plataformas tecnológicas.	P	P	P		P	P	S	P	S	S
	8	Proponer, implementar y cumplir normas de seguridad para el funcionamiento, uso y manejo de los sistemas y equipo informático, a nivel institucional.							P			

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Matriz de interrelación entre los objetivos institucionales de TI y los principios de Gobierno de TI

Principios de Gobierno de TI		Modelos de Gobierno
	1	Definir el Plan Estrategico de TI
	2	Definir la arquitectura de la información
	3	Determinar la dirección tecnológica
	4	Definir procesos, organización y relaciones de TI
Principio No. 1 Responsabilidad	5	Administrar la inversión de TI
	6	Comunicar las aspiraciones y la dirección de la gerencia
	7	Administrar recursos humanos de TI
	8	Administrar calidad
	9	Administrar y evaluar riesgos de TI
Principio No. 2 Estrategia	10	Administrar proyectos
	11	Identificar soluciones autorizadas
	12	Adquirir y mantener el software aplicativo
	13	Adquirir y mantener la infraestructura tecnológica
	14	Facilitar la operación y el uso
Principio No. 3 Adquisición	15	Adquirir recursos de TI
	16	Administrar cambios
	17	Instalar y acreditar soluciones y cambios
	18	Definir y administrar niveles de servicios
	19	Administrar servicios de terceros
Principio No. 4 Desempeño	20	Administrar desempeño y capacidad
	21	Garantizar la continuidad del servicio
	22	Garantizar la seguridad de los sistemas
	23	Identificar y asignar costos
	24	Educar y entrenar a los usuarios
Principio No. 5 Conformidad	25	Administrar la mesa de servicios y los incidentes
	26	Administrar la configuración
	27	Administrar los problemas
	28	Administrar los datos
	29	Administrar el ambiente físico
Principio No. 6 Comportamiento Humano	30	Administrar las operaciones
	31	Monitorear y evaluar el desempeño de TI
	32	Monitorear y evaluar el control interno
	33	Garantizar cumplimiento regulatorios
	34	Proporcionar gobierno de TI

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Matriz de interrelación entre los objetivos institucionales de TI y los principios de Gobierno de TI

No. de Modelo con que se relaciona	*Objetivos de TI Institucionales
2 ✓	Implementar y supervisar el funcionamiento de sistemas de telecomunicación y nuevas plataformas tecnológicas.
10	Planificar, coordinar y supervisar funciones y actividades asignadas a las, Divisiones de Desarrollo de Sistemas y de Operaciones que tiene bajo su cargo.
12	Instalar y supervisar el funcionamiento de los nuevos sistemas informáticos.
13	Analizar, diseñar, desarrollar y supervisar sistemas informáticos que apoyan los procesos de las dependencias del Instituto.
15	Formular proyectos de tecnología y gestionar la adquisición del equipo informático para implementarlos.
24	Capacitar y facilitar soporte técnico a usuarios de los sistemas informáticos.
25	Asesorar y coordinar las actividades informáticas que se desarrollan en las dependencias del Instituto.
33 ✓	Proponer, implementar y cumplir normas de seguridad para el funcionamiento, uso y manejo de los sistemas y equipo informático, a nivel institucional.

✓ ✓

Comentario

*El proceso de interrelación entre los objetivos de institucionales de TI, se basan en la comparación de las propuestas de un adecuado gobierno de la norma ISO 38500.

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Sumaria del cumplimiento del Manual de Organización, relacionada a los requerimientos mínimos de las TI

Ref. P/T	Requerimientos Mínimos de TI, que debe incluirse dentro de la Organización de las Tecnologías de la Información	Cumplimiento
C-1	Administración de los datos.	No
	Gestión de la Documentación.	No
	Plan estratégico de tecnología.	No
	Administración de proyectos de sistemas.	Si
	Infraestructura de tecnología.	No
	Relaciones con proveedores.	No
	Adquisición de tecnología.	No
	Mantenimiento de software de aplicación.	No
	Administración, desempeño, capacidad y disponibilidad de la infraestructura tecnológica.	No
	Continuidad del negocio.	No
	Seguridad de los sistemas.	Si
	Administración de operaciones de tecnología.	Si
	Cumplimiento de requerimientos legales para derechos de autor, privacidad y comercio electrónico.	No
	Educación y entrenamiento de usuarios.	No

Conclusiones:

a) Se determinó que los el manual del departamento de informática, no se alinean a las nuevos marcos de referencia de un adecuado Gobierno de TI, debido a que cuando se realizó la propuesta no se integraron los requerimientos mínimos de los principios para un adecuado Gobierno de TI, como lo indica la Norma ISO 38500.

b) La Estructura organizacional depende de la Subgerencia Administrativa por lo que no se tiene la independencia requerida para la adecuada toma de decisiones.

Por lo anterior se emitirá una observación por el área de mejora.

Elaborado por:
Christian David Sumale Chocoj, **Auditor Interno**
Fecha: 08 de febrero de 2016
Firma:

Supervisado por:
Lic. Erwin José Ericastilla López
Fecha: 12 de febrero de 2016
Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Objetivo:

Determinar la existencia de políticas y buenas prácticas incluidas en la normativa institucional que gestiona la operatividad del Departamento de informática.

Alcance:

La evaluación de la Gestión del Gobierno de Tecnologías de la Información, basado en la alineación estratégica; políticas, estándares y procedimientos.

Instituto Autónomo y Descentralizado de Salud

Manual de Organización del Departamento de Informática

MANUAL DE ORGANIZACIÓN DEL DEPARTAMENTO DE INFORMÁTICA

CFO

I. INTRODUCCIÓN

El Manual de Organización para el Departamento de Informática, es una herramienta que tiene la finalidad de ofrecer un instrumento técnico administrativo, que oriente y apoye en el desarrollo de las funciones del Departamento.

Se hace necesario que el Departamento de Informática cuente con un Manual que brinde al usuario el respaldo y ayuda necesaria en el uso de los recursos tecnológicos del Instituto, a fin de coadyuvar al logro de los objetivos de cada Departamento.

El manual detalla sistemáticamente los objetivos del Departamento, estructura organizacional, funcional y administrativa, El Departamento de Informática, delimita puestos de responsabilidad para cumplimiento de las funciones asignadas y los distribuye en las áreas internas atribuciones y responsabilidades de puestos de trabajo y organigramas.

II. OBJETIVOS DEL DEPARTAMENTO

a) Establecer un instrumento administrativo que de forma técnica contenga las bases para apoyar y facilitar la orientación de las tareas delegadas al personal que integra el Departamento de Informática y lograr un efectivo sistema de control interno. (a)

(a) **Ver análisis de literales en C-1.5/5**

b) Velar por el cumplimiento de las disposiciones legales vigentes del Instituto, que conduzcan a un manejo eficiente de la infraestructura y recursos tecnológicos, a fin de velar por la seguridad, soporte y disponibilidad de la información.

III. ESTRUCTURA ORGANIZACIONAL

CFO

El Departamento de Informática se organiza internamente para cumplir y desarrollar las funciones asignadas, en la forma siguiente:

(b)

A. JEFATURA
B. DIVISIÓN DE DESARROLLO DE SISTEMAS C. DIVISIÓN DE OPERACIONES

IV. ESTRUCTURA FUNCIONAL

A. DEPARTAMENTO DE INFORMÁTICA

a) Planificar, coordinar y supervisar funciones y actividades asignadas a las Divisiones de Desarrollo de Sistemas y de Operaciones que tiene bajo su cargo.
b) Analizar, diseñar, desarrollar y supervisar sistemas informáticos que apoyan los procesos de las dependencias del Instituto.
c) Implementar y supervisar el funcionamiento de sistemas de telecomunicación y nuevas plataformas tecnológicas.
d) Instalar y supervisar el funcionamiento de los nuevos sistemas informáticos.
e) Formular proyectos de tecnología y gestionar la adquisición del equipo informático para implementarlos.
f) Capacitar y facilitar soporte técnico a usuarios de los sistemas informáticos.
g) Asesorar y coordinar las actividades informáticas que se desarrollan en las dependencias del Instituto.

(b) **Ver análisis de literales en C-1.5/5**

h) Proponer, implementar y cumplir normas de seguridad para el funcionamiento, uso y manejo de los sistemas y equipo informático, a nivel institucional.

V. ESTRUCTURA ADMINISTRATIVA

CFO

A. JEFATURA

1. Jefe del Departamento (C)

1.1 Subjefe

1.2 Secretaria

1.3 Responsable de Presupuesto

B. DIVISIÓN DE DESARROLLO DE SISTEMAS

1. Coordinador de Desarrollo de Sistemas

1.1 Programadores

2. Responsables de Recepción de Aplicaciones

3. Responsables de Pruebas e Implementación

4. Responsable de Control de Calidad

C. DIVISIÓN DE OPERACIONES

1. Jefe de Grabación y Operaciones

1.1 Técnicos Operadores

2. Jefe de Soporte Técnico

(C) **Ver análisis de literales en C-1.5/5**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

CFO

2.1 Técnicos de Soporte Nivel1

2.2 Técnicos de Soporte Nivel 2

3. Responsables de Base de Datos

4. Responsable de Arquitectura de Software

5. Responsable de Administración de Página Web

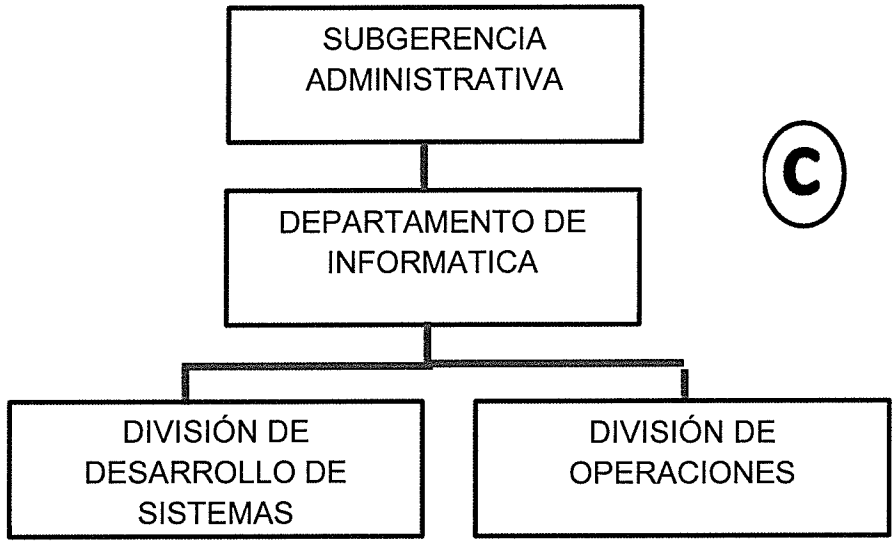
5.1 Diseñador de Página Web

6. Responsables de Plataforma Tecnológica

7. Responsables de Telecomunicaciones

8. Responsable de Auditoría de Sistemas

VI. ORGANIGRAMA



C

(c) Ver análisis de literales en C-1.5/5

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Observaciones a la normativa:

Literales

(a) Del análisis a la presente normativa se puede determinar que los el manual del departamento de informática, no se alinean a las nuevos marcos de referencia de un adecuado Gobierno de TI, debido a que cuando se realizó la propuesta no se integraron los principios para un adecuado Gobierno de TI.

(b) Se estableció que en la mayoría de atribuciones que se detallan en la resolución antes descrita la Jefatura del departamento de informática carecen de una visión moderna apegada a un marco de referencia y que en su mayoría no son atendidos por el jefe ya que se le ha nombrado como director de proyectos por lo que no puede cumplir con dichas atribuciones debido a que se determinó que el Licenciado Sergio Gerardo Diéguez Fajardo no es el titular de la plaza de jefe del departamento de informática sino simplemente está cubriendo la misma de manera interina.

(c) La Estructura organizacional depende de la Subgerencia Administrativa por lo que no se tiene la independencia requerida para la adecuada toma de decisiones.

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Sumaria de la evaluación de la continuidad de servicio de las Tecnologías de la Información

Ref. P/T	Factor de riesgo para la continuidad de los Servicios de TI, dentro de la Institución*	Ocurrencia ☐
D-1	Mal funcionamiento de hardware o software. ❮	Recurrente
	Compras innecesarias. ❙	Poca Ocurrencia
	Falta de personal calificado para el manejo de los nuevos sistemas. ❮	Recurrente

- Se estableció la falta de una adecuada renovación de activos tecnológicos, debido a que no se ha podido realizar la adquisición de nuevas licencias que permita mejorar la conectividad al poner en funcionamiento los appliance.

Por lo anterior se emitirá una observación por el área de mejora.

☐ Ver en criterios de ocurrencia en **Cédula de Criterio de Ocurrencia.**

* Factor de Riesgos obtenido de las entrevistas a funcionarios y personal clave

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 15 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 18 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula Narrativa de procesos de continuidad de servicio de las Tecnologías de la Información

Objetivo:

Obtener evidencia si existe política que permitan gestionar de una manera adecuada la continuidad de los servicios prestados por la institución.

Alcance:

Evaluar la continuidad de los servicio de las Tecnologías de la Información

Persona a Entrevistar: Jefe del Departamento de Informática

El inconveniente que afecta la continuidad de los servicios que presta la institución es la falta de licencias de los dispositivos de asignación de direcciones IP (appliance) que se utilizan para mejorar la conectividad con el Internet que proporciona el proveedor, pero el evento de adquisición de dichas licencias se ha gestionado de manera lenta, y se han priorizado compras que no son tan elementales para la continuidad de los servicios de TI; así mismo, se ha tenido el inconveniente de falta de personal calificado para resolver problemas con los appliance.

F. **F.**

Persona Encuestada **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Sumaria de la evaluación de las competencias del personal del Departamento de Informática

Ref. P/T	Factor de riesgo en la competencia del personal del Departamento de informática*	Ocurrencia ☐
E-1	Falta de tecnificación del personal.	Recurrente
	Perfiles no definidos para la contratación del personal.	Poca Ocurrencia
	Falta de capacitaciones.	Recurrente

Conclusión:

Se estableció al evaluar la competencia del personal que se cuentan con perfiles definidos pero estos no son actualizados frecuentemente, se capacita al personal del departamento de informática; así mismo, se evalúa cada año para determinar sus competencias. Por lo anterior se emitirá una observación por el área de mejora.

☐ Ver en criterios de ocurrencia en **Cédula de Criterio de Ocurrencia**.

* Factor de Riesgos obtenido de las entrevistas a funcionarios y personal clave

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 15 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 18 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula narrativa de procedimientos para la selección y capacitación del Personal del Departamento de informática

Objetivo:

Obtener evidencia si el personal del Departamento de Informática cumple con los conocimientos necesarios para desempeñar las actividades inherentes a este.

Alcance:

La gestión sobre el recurso humano y las directrices de Gobierno emitidas para el efecto

Persona a Entrevistar: Jefe del Departamento de Informática

El Departamento de Informática solicita a la Subgerencia de Recursos Humanos la dotación del personal idóneo que pueda desempeñar las atribuciones que se requieren dentro del Departamento, a lo cual dicha Subgerencia en ciertas ocasiones ha comentado, que es imposible poder dotar del personal requerido, debido a que los salarios que la institución ofrece a los postulantes, son demasiado bajos para la actividades que desempeñaran, por lo que las contrataciones se realizan sin prestaciones de ley, lo que permite poder aumentar la cantidad que devengan haciendo más atractivo las remuneraciones, en cuanto a las capacitaciones se contempló la realización para tener personal calificado que pueda resolver los inconvenientes que se suscitan dentro del departamento; así mismo, se realiza una evaluación de desempeño anualmente para determinar la calidad del personal.

F. **Persona Encuestada**

F. **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Persona a Entrevistar: Subgerente de Recursos Humanos

Dentro de la institución se hace un poco difícil la administración del recurso humano, debido a la cantidad de empleados que posee la institución, contratados en distintos renglones, efectivamente se cuentan con perfiles definidos para la contratación de dicho personal, el inconveniente que se tienen con esto es la falta de actualización, debido a que los perfiles definidos por Gerencia y aprobados por la honorable Junta Directiva, no son actualizados frecuentemente, derivado de esa situación se cuentan con perfiles que en su mayoría cubre los aspectos más básicos para la contratación, en cuanto a la capacitación del personal del Departamento de Informática, se da apoyo coordinando dichas actividades; asimismo, se coloca a disposición de este departamento becas y diplomados con entidades de educación superior para la tecnificación de dicho personal. Dentro del apoyo que se brinda al departamento de informática se contempla anualmente evaluaciones de desempeño que orientan a la jefatura de dicho departamento si efectivamente cuenta con personal calificado para desempeñar adecuadamente las funciones inherentes a la gestión de TI.

F. **F.**

Persona Encuestada **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula narrativa de procedimientos sobre directrices de Gobierno de la gestión de infraestructuras y aplicaciones de Tecnologías de Información

Objetivo:

Obtener evidencia si existen políticas para salvaguardar la integridad de los activos tecnológicos.

Alcance:

Las directrices de Gobierno sobre la gestión de infraestructuras y aplicaciones de Tecnologías de Información.

Persona a Entrevistar: Jefe del Departamento de informática

Se entrevistó al jefe del departamento de informática en cuanto a las políticas que se implementaron para salvaguardar la integridad de los activos tecnológicos por lo que se estableció que se cuenta con un manual de procedimientos del departamento de informática para el manejo y administración de los activos tecnológicos, el cual se basó en buenas practicas que establece la norma ISO 27001 y 27002, en cuanto a la seguridad física de los activos, la administración, organización. Por lo anterior revisamos el manual y lo comparamos con la norma ISO correspondiente encontrando que efectivamente cumple con ello.

Comentario:

Se estableció que efectivamente se cumple con salvaguardar los activos tecnológicos de la institución, mismo que esta normado y aplica sanciones por el incumpliendo de dicha normativa.

F. **F.**

Persona Encuestada **Auditor Interno**

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Cédula narrativa de procedimientos sobre decisiones de alto nivel que permitan contar con una seguridad razonable en la protección y disponibilidad de datos

Objetivo:

Obtener evidencia del grado de madurez referente al Gobierno de Tecnología de la Información, con que cuenta la institución.

Alcance:

Las decisiones de alto nivel que permitan contar con una seguridad razonable en la protección y disponibilidad de datos.

Trabajo realizado:

Se estructuro la matriz de medición del grado de madurez propuesta por la ISO 38500 del gobierno de tecnologías de la información, las preguntas se dividen por principio y sus estatutos con una ponderación de 0 a 5, siendo 0 la falta de madurez y 5 el nivel más alto deseado y que engloba una correcta gestión de TI.

Las matrices estructuras para la evaluación se muestran en los papeles de trabajos **G-1.1/7 al G-1.7/7**

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha 12 de febrero de 2016

Firma:

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.2 Principio 1: Responsabilidad	Evaluar	En general, los individuos o grupos dentro de la organización no tienen claras sus responsabilidades con respecto al suministro y a la demanda de la información.	Los directores de TI establecer reglas y responsabilidades con relación al uso actual y futuro de la tecnología de la información de la organización.	Con respecto al suministro y a la demanda de la información, los usuarios dentro de la organización, entienden y aceptan las reglas y responsabilidades asignadas por TI.	Los directores de TI tienen alineadas las reglas y responsabilidades con los objetivos actuales y futuros del negocio. Los niveles de entendimiento y aceptación por parte de los usuarios, con respecto al uso de la información, se encuentran documentados	Los directores de TI, evalúan la competencia (capacidad, autoridad, experiencia, etc.) de aquellos a quienes se les asigna la responsabilidad de tomar decisiones con respecto a TI. (Los resultados de estas evaluaciones se encuentran documentados)	2	5
	Dirigir	En la organización no se cuenta con proyectos de tecnología.	Los directores de TI, conocen pero no dirigen los proyectos de tecnología que se establecen en la alta gerencia de la organización (u otras áreas)	Los directores de TI dirigen todos los proyectos de tecnología de la organización. Los Directores de TI, cuentan con una autoridad parcial para solicitar información de otras dependencias.	Los directores de TI cuentan con un procedimiento documentado para ayudar a evaluar el cumplimiento de las metas de los proyectos de tecnología que dirigen.	Los directores de TI verifican que todos los proyectos de tecnología, estén alineadas con las responsabilidades asignadas al área de TI Los directores de TI exigen que se les entregue la información que necesitan para cumplir sus responsabilidades, incluidas las relativas a acciones y toma de decisiones.	2	5
	Controlar	Los directores de TI tienen algún conocimiento acerca de gobierno de TI.	Los directores de TI conocen y supervisan que se hayan establecido los mecanismos adecuados para el gobierno de TI. Así mismo, cuenta con procedimientos y/o formatos que garanticen el mantenimiento de un modelo de gobierno de TI	Los directores de TI supervisan y/o auditan periódicamente el funcionamiento de los mecanismos implementados para el cumplimiento de gobierno de TI. (Dichas supervisiones se encuentran documentadas)	Los directores de TI supervisan y/o auditan periódicamente el desempeño de aquellos a quienes se ha asignado responsabilidad en el gobierno de TI (por ejemplo, aquellas personas miembros de los comités, jefes, coordinadores, etc.)	También supervisan y/o auditan periódicamente que los individuos o grupos dentro de la organización entiendan y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de tecnología de la información.	1	4

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación del nivel de madurez

Periodo de 01 de enero al 31 de diciembre de 2015

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.3 Principio 2: Estrategia	Evaluar	Los directores de TI, evalúan y brindan soporte a las necesidades actuales del negocio.	Los directores de TI estudian los avances de la tecnología de la información y los procesos del negocio con el fin de asegurarse de que TI brinda soporte a las necesidades futuras del negocio. (Los resultados de dicha evaluación se encuentran documentadas)	Los directores de TI evalúan y monitorean las actividades de TI, pero no aseguran que estas se mantengan (con el paso del tiempo) alineadas con los objetivos de la organización.	Los directores de TI cuentan con un plan estratégico de TI, el cual tiene en cuenta los planes y las políticas de la organización. Los directores de TI evalúan periódicamente que las actividades de TI se mantengan alineadas con los objetivos de la organización. (Los resultados de dicha evaluación y alineación con los objetivos de la organización se encuentran documentados)	Los directores de TI garantizan que sus procesos podrían ser (en cualquier momento), verificados, auditados y/o evaluados tal como se describe en normas nacionales e internacionales pertinentes.	1	4
	Dirigir	Los usuarios conocen los procesos de TI de la Organización.	Los usuarios de la Organización están autorizados para presentar propuestas de innovación para TI	La Organización fomenta y estimula la presentación de propuestas de innovación de TI (Se tiene establecido un procedimiento, formato lineamiento, etc., que evidencie la forma como se fomenta dicha actividad)	Los directores de TI tienen establecidos procedimientos y/o formatos para la presentación y recepción de propuestas de innovación en TI.	Los directores de TI fomentan y evalúan que estas propuestas permitan a la organización responder a oportunidades, nuevos retos, mejorar los procesos de la organización y/o estén alineadas con los objetivos del negocio.	2	4
	Controlar	La Organización cuenta con una metodología para la ejecución de proyectos	Todos los proyectos de la organización (incluidos los de TI) son monitoreados para supervisar el progreso de los mismas	Los directores de TI conocen y supervisan el progreso de los proyectos de TI (Dicha supervisión se encuentra debidamente documentada)	Los directores de TI no solo supervisan el progreso del avance de los proyectos de TI, sino que se asegura que se estén cumpliendo los objetivos y beneficios planteados.	Los directores de TI, supervisan el uso de TI para asegurar que de ésta, se obtienen los beneficios previstos y que continúen alineados con los objetivos de la organización.	2	5

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.4 Principio 3: Adquisición	Evaluar	Cualquier proceso dentro de la Organización puede solicitar un requerimiento para la adquisición tecnología.	Los directores de TI evalúan diferentes opciones al momento de adquirir tecnología, pero no son los únicos encargados de aprobar la propuesta.	Los directores de TI son los encargados y responsables adquirir tecnología para la organización	Los directores de TI aprueban la mejor propuesta que de cumplimiento a los requerimientos planteados, además que garantice el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo.	Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento del equilibrio mencionado	2	4
	Dirigir	Los directores de TI gestionan y mantienen los activos de TI (sistemas e infraestructura)	Los directores de TI adquieren tecnología de forma correcta, clara y transparente, teniendo en cuenta los requerimientos planteados	Los directores de TI verifican que se incluya la respectiva documentación (instructivos, manuales, etc.) de la tecnología adquirida, a la vez que aseguran que el las tecnologías adquiridas cumplen con las capacidades requeridas.	Los directores de TI verifican el cumplimiento de los acuerdos de nivel de servicio (tanto internos como externos)	Los directores de TI gestionan los acuerdos de nivel de servicio (tanto internos como externos) de modo que aseguran que estos soportan las necesidades del negocio. (Se cuenta con un procedimiento documentado y/o formatos que evidencien el cumplimiento de los acuerdos de nivel de servicio)	0	5
	Controlar	La organización cuenta con mecanismos para supervisar que las inversiones, en términos generales, están acordes con las requeridas.	Los directores de TI supervisan (auditan) que las inversiones en TI, proporcionan las capacidades requeridas para las cuales fueron adquiridas.	Se tienen algún tipo de procedimiento y/o formato que permita evidenciar el resultado de la supervisión realizada en las inversiones de TI	Los directores de TI tienen contacto con los proveedores de tecnología solo en ocasiones puntuales	Los directores de TI tienen contacto y/o alianzas estratégicas con los todos los proveedores de tecnología.	1	4

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.5 Principio 4: Desempeño	Evaluar	Los directores de TI evalúan que la tecnología de la información apoya los procesos de negocio con la habilidad y capacidad requeridas.	Los directores de TI tienen políticas dirigidas hacia la continuidad de la operación normal del negocio y del tratamiento de los riesgos asociados con el uso de la tecnología de la información.	Los directores de TI evalúan periódicamente los riesgos que se originan en las actividades de la tecnología de la información para la continuidad de la operación de los negocios. Además evalúan los riesgos para la integridad de la información y protección de los activos de tecnología de la información, incluyendo la propiedad intelectual y memoria organizacional asociadas.	Los directores de TI garantizan que la tecnología de la información es adecuada para brindar soporte a la organización, suministrando los servicios, los acuerdos de niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio, soportando las metas del negocio.	Los directores de TI evalúan con regularidad la eficacia y el desempeño del sistema organización para el gobierno TI (Se cuenta con un procedimiento documentado y/o formatos que evidencia el cumplimiento de esta evaluación)	2	4
	Dirigir	La Organización cuenta con un mecanismo de asignación de recursos para sus diferentes procesos.	Los directores de TI tienen asegurada la asignación de los recursos suficientes para el ejercicio de sus funciones	Los directores de TI garantizan que los recursos que le son asignados, satisfacen las necesidades de la organización.	La información que soporta al negocio, se encuentra disponible cuando se requiere, con datos correctos y actualizados y están protegidos contra pérdida o mal uso.	Los directores de Ti cuentan con mecanismos y/o procedimientos que garantizan la calidad y disponibilidad de la información	2	5
	Controlar	Los directores de TI supervisan la "vida útil" de la tecnología de la información da soporte al negocio.	Los directores de TI cuentan con mecanismos documentados que permiten prever cuando la tecnología de la información, se acerca al final de su "vida útil"	Se tiene establecido un cronograma, el cual se encuentra supervisado, de renovación de la tecnología de la información, de igual forma se tiene asegurado los recursos para dicha renovación.	Los directores de TI poseen, controlan y supervisan el presupuesto asignado por la Organización para la inversión de TI	Los directores de TI dan prioridad a las inversiones que impacten directamente los objetivos del negocio.	0	5

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.6 Principio 5: Conformidad	Evaluar	Los directores de TI garantizan que la tecnología de la Información cumple con todos lineamientos establecidos por la Organización	De igual manera, los directores de TI garantizan que la tecnología de la Información de la Organización cumple con todas las leyes y los reglamentos obligatorios.	La Organización cuenta con políticas y prácticas claras, las cuales se encuentran documentadas y detallan los requerimientos legales de TI que rigen a la Organización.	Los directores de TI supervisan periódicamente que se cumplen dichas prácticas y políticas expresadas por la Organización.	Los directores de TI evalúan periódicamente que las tecnologías de la información satisfacen las obligaciones reglamentarias, legislativas, de ley, contractuales, las políticas internas, las normas y las directrices profesionales.	1	5
	Dirigir	La Organización garantiza que se cumple con las obligaciones legales pertinentes.	Los directores de TI colaboran con la Alta Gerencia a establecer mecanismos regulares y rutinarios para garantizar que el uso de la tecnología de la información cumple con las obligaciones pertinentes (reglamentarias, legislativas, de ley, contractuales), las normas y las directrices.	Los directores de TI supervisan periódicamente que se cumpla con las obligaciones internas y externas en el uso de la tecnología de la información.	Los resultados de estas supervisiones se encuentran documentadas y son analizadas periódicamente en busca de la mejora continua.	La organización cuenta con directrices claras que regulan el comportamiento de los usuarios con relación a las TI de la Organización.	5	5
	Controlar	Los directores de TI supervisan la conformidad y el cumplimiento de las obligaciones de TI a través de prácticas adecuadas de auditoria.	Dichas auditorias se encuentran debidamente programadas, son oportunas, exhaustivas y adecuadas y evalúan el grado de satisfacción de las tecnologías de la información con los objetivos, políticas y/o directrices de la Organización	Las auditorias incluyen la supervisión de los activos de TI y los datos (información) de la Organización.	También se incluye la verificación del cumplimiento de todas las obligaciones legales pertinentes y las suscritas con clientes y proveedores	Las auditorias también supervisan las actividades tendientes a la preservación de la información privada de la Organización	1	5

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Apartado		Nivel de Madurez					Escriba su nivel actual	Escriba su nivel deseado
		Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5		
3.7 Principio 6: Comportamientos Humanos	Evaluar	Los usuarios de la Organización tienen un conocimiento básico de las tecnologías que tienen disponibles	Los directores de TI ayudan a que los usuarios entiendan y aprovechen la tecnología que tienen disponible, de modo que estos aumenten su desempeño personal y el de los sistemas de información.	Los directores de TI tienen documentadas las interacciones (relaciones) existentes entre los usuarios y las tecnologías de la información disponibles en la Organización.	La Organización conoce acerca del comportamiento humano y sabe que esto incluye: La cultura, las necesidades, y las aspiraciones de los usuarios, bien sea como individuos o como grupos. Además, los directores de TI son conscientes (y lo documentan como un riesgo) que estos comportamientos humanos pueden afectar el rendimiento las tecnologías de la información	Las políticas, prácticas y decisiones con respecto a TI demuestran respeto por el comportamiento humano.	1	5
	Dirigir	Los directores de TI dirigen de tal manera que las actividades de TI sean consistentes con el comportamiento humano identificado.	Los directores de TI cuentan con mecanismos que permiten que cualquier persona en cualquier momento pueda identificar y reportar riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información	La Organización cuenta con políticas y/o procedimientos que permiten escalar los riegos reportados hasta las personas correspondientes a cargo de la toma de decisiones.	Todos los reportes acerca de los riesgos, oportunidades, problemas y preocupaciones relacionados con las tecnologías de la información, se encuentran debidamente documentados	Los directores de TI analizan periódicamente todos los reportes generados en busca de mejoras para la Organización	0	5
	Controlar	La Organización supervisa periódicamente el nivel de satisfacción del comportamiento humano. (Por medio de encuestas de clima laboral, por ejemplo).	La Organización analiza los resultados de la supervisión de los comportamientos humanos y brinda la atención adecuada que se requiera para mejorar nivel de satisfacción.	Los directores de TI supervisan periódicamente cómo los comportamientos humanos afectan el rendimiento de las tecnologías de la información.	La Organización supervisa periódicamente que las políticas, prácticas y decisiones de TI demuestren respeto por el comportamiento humano	Los directores de TI supervisan las prácticas laborales de los usuarios, con el fin de asegurar que sean consistentes del uso adecuado de la tecnología de información.	0	5

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 15 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha: 18 de febrero de 2016

Firma:

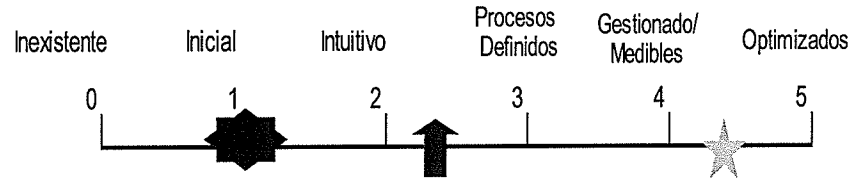
Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Periodo de 01 de enero al 31 de diciembre de 2015

Comentario:

Se estableció que derivado de la evaluación al grado de madurez del gobierno de TI, que la institución cuenta con un Gobierno de Tecnologías de la Información inicial, con principios establecidos, pero procesos desorganizados, lo anterior debido a la falta de políticas y normativa que concentren todos los principios de un adecuado Gobierno de TI. El resumen de la evaluación se resume a continuación:



Estado actual de la entidad

Media

Valor objetivo de la entidad

0 - La entidad no conoce el principio, no es consciente de necesitarlo
1 - Principio establecido, pero procesos desorganizados y son *ad hoc*
2 - Principio inmaduro, los procesos siguen un patrón regular
3 - Principio comienza a madurar, procesos documentados y comunicados
4 - Principio bastante maduro, los procesos se monitorizan y se miden
5 - Principio a nivel optimo , basado en buenas prácticas

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha 12 de febrero de 2016

Firma:

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Cédula de Marcas

Periodo de 01 de enero al 31 de diciembre de 2015

√	Verificado con Modelo de Gobierno de la Norma ISO 38500
√	Verificado con el Plan Estratégico Institucional
√1	Verificado con Objetivos de TI
❮	Niveles de Madurez
⬟	Criterio de Probabilidad
Δ	Criterios del Modelo de Madurez
□	Criterios de Ocurrencia
CFO	Copia Fiel de la Original
PT	Papel de trabajo

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Cédula de Criterio de Grado de Conocimiento del Gobierno de TI

Periodo de Evaluación del 01 de enero al 31 de diciembre de 2015

Orden	Criterio	Descripción
1	Alto	Conoce de los principios para la Gestión de un adecuado Gobierno de TI.
2	Medio	Probablemente conoce algunos principios de Gobierno de TI.
3	Bajo	Casi improbable que conozca los principios de Gobierno de TI.

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha 12 de febrero de 2016

Firma:

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Cédula de Criterio de Ocurrencia

Periodo de Evaluación del 01 de enero al 31 de diciembre de 2015

Orden	Criterio	Descripción
1	Recurrente	Se muestra una tendencia constante de que se dé la deficiencia.
2	Poca Ocurrencia	Poco probablemente que se dé la deficiencia.

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 08 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha 12 de febrero de 2016

Firma:

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

Instituto Autónomo y Descentralizado de Salud

Evaluación de Gobierno de TI

Cedula de Niveles de Madurez

Periodo de Evaluación del 01 de enero al 31 de diciembre de 2015

Nivel	Descripción
0	La entidad no conoce el principio, no es consciente de necesitarlo
1	Principio establecido, pero procesos desorganizados y son *ad hoc*
2	Principio inmaduro, los procesos siguen un patrón regular
3	Principio comienza a madurar, procesos documentados y comunicados
4	Principio bastante maduro, los procesos se monitorizan y se miden
5	Principio a nivel óptimo , basado en buenas prácticas

Elaborado por:

Christian David Sumale Chocoj, **Auditor Interno**

Fecha: 15 de febrero de 2016

Firma:

Supervisado por:

Lic. Erwin José Ericastilla López

Fecha 18 de febrero de 2016

Firma:

4.10 Informe de Auditoría

DEPARTAMENTO DE AUDITORÍA INTERNA

INSTITUTO AUTÓNOMO Y DESCENTRALIZADO DE SALUD

ENTIDAD	Instituto Autónomo y Descentralizado de Salud
TIPO DE AUDITORÍA	Auditoría informática
PERÍODO	Del 01 de enero al 31 de diciembre de 2015

Guatemala, febrero de 2016

Guatemala, 29 de febrero de 2016

Licenciado
Sergio Armando Diéguez Solórzano
Gerente
Instituto Autónomo y Descentralizado de Salud
Su Despacho

Atentamente me dirijo a usted, con el propósito de presentar el informe de la evaluación al Gobierno de Tecnologías de la Información practicado al Instituto, nuestro alcance fue: la alineación estratégica del Gobierno de Tecnologías de la Información; políticas, estándares y procedimientos; la continuidad de los servicio de las Tecnologías de la Información; gestión sobre el recurso humano y las directrices de Gobierno emitidas para el efecto; así como, la gestión de infraestructuras y aplicaciones de Tecnologías de Información y las decisiones de alto nivel que permitan contar con una seguridad razonable en la protección y disponibilidad de datos, correspondiente al periodo del 1 de enero al 31 de diciembre de 2015.

De acuerdo a la evaluación realizada al Gobierno de Tecnologías de la Información se puedo establecer que la institución cuenta con un Gobierno de Tecnologías de la Información inicial, con principios establecidos, los que carecen de procesos organizados, debido a la falta de políticas y normativa que concentren todos los principios de un adecuado Gobierno de TI.

Todos los comentarios y recomendaciones que hemos detectado, se encuentran en detalle en el correspondiente informe de auditoría, lo cual facilitará un mejor entendimiento de este resumen gerencial.

La evaluación, fue realizada por el Asistente de Auditoría Interna Christian David Sumale Chocoj.

Deferentemente,

Licenciado Erwin José Ericastilla López
Jefe del Departamento de Auditoría Interna

1. ANTECEDENTES

El Instituto Autónomo y Descentralizado de Salud creado 30 de octubre de 1946 inicia como una consecuencia de la segunda guerra mundial y la difusión de ideas democráticas en el mundo, el 20 de octubre de 1944 se derrocó al gobierno del General Federico Ponce Vaides y se eligió un gobierno democrático, bajo la presidencia del Doctor Juan José Arévalo. El Gobierno de Guatemala de aquella época, gestionó la venida al país de dos técnicos en materia de Salud, quienes hicieron un estudio de las condiciones económicas, geográficas, étnicas y culturales de Guatemala. Al promulgarse la Constitución de la República de aquel entonces, el pueblo de Guatemala, encontró entre las Garantías Sociales, "UN RÉGIMEN NACIONAL, UNITARIO Y OBLIGATORIO DE SALUD, DE CONFORMIDAD CON EL SISTEMA DE PROTECCIÓN MÍNIMA". La Ley regulaba sus alcances, extensión y la forma en que debía ser puesto en vigor. El 30 de octubre de 1946, el Congreso de la República de Guatemala, emite el Decreto número 296. Creando así "Una Institución autónoma, de derecho público de personería jurídica propia y plena capacidad para adquirir derechos y contraer obligaciones, cuya finalidad es aplicar en beneficio del pueblo de Guatemala, un régimen nacional, unitario y obligatorio de salud, de conformidad con el sistema de protección mínima". Un régimen nacional, unitario y obligatorio, esto significa que debe cubrir todo el territorio de la República, debía ser único para evitar la duplicación de esfuerzos y de cargas tributarias, sin evadir sus obligaciones, pues ello significaría incurrir en la falta de salud.

2. ALCANCE

El alcance del trabajo a realizar será la evaluación de la Gestión del Gobierno de Tecnologías de la Información, basado en la alineación estratégica; políticas, estándares y procedimientos; la continuidad de los servicio de las Tecnologías de la Información; gestión sobre el recurso humano y las directrices de Gobierno emitidas para el efecto; así como, la gestión de infraestructuras y aplicaciones de Tecnologías de Información y las decisiones de alto nivel que permitan contar con

una seguridad razonable en la protección y disponibilidad de datos, que comprende el periodo del 01 de enero al 31 de diciembre 2015.

3. DICTAMEN

De acuerdo a la evaluación realizada al Gobierno de Tecnologías de la Información se puedo establecer que la institución cuenta con un Gobierno de Tecnologías de la Información inicial, con principios establecidos, los que carecen de procesos organizados, debido a la falta de políticas y normativa que concentren todos los principios de un adecuado Gobierno de TI.

4. HALLAZGOS RELACIONADOS CON EL GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

Hallazgo No. 1

Deficiente Estructura Organizacional

La estructura organizacional y operacional del Departamento de Informática no se alinea en función de su composición y ámbito de decisiones y no existe independencia ni un criterio objetivo, que permita una adecuada supervisión, gestión y administración de los activos tecnológicos, lo anterior a que depende jerárquicamente de la Subgerencia Administrativa.

Criterio

COBIT 5 "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa"

En cada empresa, se definen varias estructuras organizativas; en función de su composición y ámbito de decisiones, las estructuras pueden ubicarse en el área de gobierno o en el de gestión. Dado que el gobierno trata acerca de establecer la orientación, la interacción tiene lugar entre las decisiones tomadas por las estructuras de gobierno.

Causa

Falta de una estructura independiente del Departamento de Informática con una adecuada segregación de funciones.

Efecto

Inadecuada toma de decisiones, debido a la falta de una estructura adecuada, que permita establecer instrucción que permitan alcanzar los objetivos institucionales, con eficiencia y eficacia.

Comentario de la Administración

Los problemas de la conformación de la estructura organizativa dentro de la institución ha sido por años un problema que tanto la Junta Directiva como la Gerencia, han tratado de mitigar, en el que no han tenido éxito, por la falta de involucramiento de todos los niveles a quienes les compete, indicar si la estructura propuesta es la más adecuada o si la misma debe actualizarse, por otra parte los distintos factores externos que amenazan la estabilidad institucional, es la causa principal que se priorice en atender a los pacientes que asisten a la institución y se dejan de lado proyectos que permitirán mejorar la atención.

Recomendación

Que sea creado dentro de la máxima autoridad de la institución una comisión que gestión, actualice y cree la estructura organizacional relacionada a las tecnologías de la información, que proporcione una base de referencia para la gestión objetiva de la gobernanza corporativa de la TI.

Hallazgo No. 2

Disociación de los objetivos institucionales y los objetivos de TI

Los objetivos estratégicos institucionales y los objetivos de TI, carecen de una alineación, planificación y organización objetiva, al comparar los objetivos de TI de la Institución con el modelo de gobierno propuesto por la Norma ISO 38500,

basado en los principios de un adecuado Gobierno de TI, la institución contempla únicamente ocho de treinta y tres propuestas, que garantizan una adecuada gestión de TI.

Criterio

Principios de la Norma ISO 38500 "principio 2 estrategia": la planificación estratégica de la TI es una tarea compleja y crítica que requiere una estrecha coordinación entre la unidad de negocio de la empresa y los planes estratégicos de las TI. También es vital priorizar los planes que mejor se adecúan a la consecución de los beneficios deseados y a asignar eficazmente los recursos. Los logros de alto nivel tienen que ser traducidos a planes tácticos realizables, garantizando los mínimos fallos y sorpresas. La meta es conferir valor en el apoyo de los objetivos estratégicos a la vez que se tiene en cuenta el riesgo asociado en relación al umbral de riesgo del consejo.

Causa

Falta de procedimientos documentados que regulen la formulación adecuada del Plan Estratégico Institucional.

Efecto

Riesgo del incumplimiento de metas por la falta de cumplimiento de los objetivos estratégicos.

Comentario de la Administración

Los objetivos estratégicos institucionales y los objetivos de TI, efectivamente no están alineados, esto debido a que en recientes fechas fueron actualizados los objetivos estratégicos por la máxima autoridad de la institución, con esta actualización se pretende mejorar la calidad de los servicios que presta esta institución a la población Guatemalteca.

Recomendación

Que se formule y alineen de acuerdo a un marco de referencia integral los objetivos estratégicos y los objetivos de TI, priorizando los planes tácticos realizables que garanticen valor en el apoyo de los objetivos estratégicos, que mejor se adecúan a la consecución de los beneficios deseados y a asignar eficazmente los recursos, minimizando fallos y sorpresas, dentro de la Institución.

Hallazgo No. 3

Falta de comunicación entre el personal involucrado en la gestión del Gobierno de TI

Al analizar las entrevistas que se practicaron al personal clave, se estableció que existe falta de comunicación entre la alta dirección y el personal involucrado en la gestión del Gobierno de TI, debido a que la Junta Directiva tiene contemplado proyectos relacionados con la actualización de la plataforma informática que no han sido comunicados al Jefe del Departamento de Informática.

Criterio

Catalizador de COBIT 5: Cultura, Ética y Comportamiento "Buenas prácticas"

Para crear, fomentar y mantener los comportamientos deseados a lo largo de toda empresa incluyen:
Comunicación a lo largo de toda la empresa de los comportamientos deseados y los valores corporativos subyacentes.

Causa

Falta de políticas orientadas a la aplicación de una comunicación efectiva que permita a todo el personal involucrado, empoderarse de los proyectos y en consecuencia cuenten con la información necesaria para tomar decisiones que estén alineadas a los objetivos institucionales.

Efecto

Riesgo de duplicidad de esfuerzos y gastos innecesarios, derivados de la implementación de acciones que no coinciden con los proyectos contemplados por la alta dirección.

Comentario de la Administración

Efectivamente la institución no cuenta con políticas de comunicación entre las dependencias relacionadas a TI, en consecuencia los proyectos que se tiene contemplados, son comunicados a un nivel gerencial y no a todo el personal involucrado.

Recomendación

Que se implemente una política de comunicación a todo nivel, que permita mejorar la transmisión de instrucciones de los cuerpos de Gobierno y de dirección que permitan alcanzar los objetivos estratégicos institucionales y de TI.

Hallazgo No. 4

Falta de actualización de Perfiles de Contratación

La institución carece de perfiles actualizados, definidos para la contratación del personal del Departamento de Informática.

Criterio

Principio 6: Conducta Humana ISO 38500 Las políticas de TI, prácticas y decisiones relacionadas con las TI muestran respeto hacia la conducta humana incluyendo las necesidades actuales y futuras de todas las "personas implicadas en el proceso".

Causa

Falta de políticas institucionales que definan las necesidades de contratación del recurso humano que se encuentra incluido en los procesos de TI.

Efecto

Riesgo errores significativos que perjudiquen la integridad de los activos tecnológicos; así como de la información que se genera en el Departamento de Informática.

Comentario de la Administración

Se considera la actualización de los perfiles definidos para la contratación de personal adecuado que ocupe los puestos que se incluyen en los procesos de gestión de las TI, sin embargo es algo complejo debido a que la Junta Directiva Institucional es quien modifica los perfiles definidos.

Recomendación

Que se actualicen los perfiles para la contratación del personal del Departamento de Informática, con base a buenas prácticas y marcos de referencias que permitan obtener recurso humano calificado que ejecute adecuadamente los procesos del Departamento de Informática.

Hallazgo No. 5

Falta de políticas de renovación de activos tecnológicos

Inadecuada renovación de activos tecnológicos, debido a que no se ha podido realizar la adquisición de nuevas licencias que permita mejorar la conectividad al poner en funcionamiento los dispositivos de asignación de direcciones IP (appliance).

Criterio

Principio 3 Adquisición de la Norma ISO 38500

Las adquisiciones de TI se hacen por razones válidas, sobre la base de análisis adecuados y continuados, a través de decisiones claras y transparentes. Hay un adecuado equilibrio entre beneficios, oportunidades, costes y riesgos, tanto a corto como a largo plazo.

Causa

Falta de políticas institucionales que definan una oportuna renovación de activos tecnológicos, para garantizar una adecuada continuidad de los servicios que presta la institución.

Efecto

Riesgo de deficiencia en las operaciones de la institución por la falta de un adecuado funcionamiento de los activos tecnológicos institucionales.

Comentario de la Administración

Se han realizado esfuerzos para realizar la adquisición de las licencias que podrían en funcionamientos los dispositivos de asignación de direcciones IP (appliance), pero la adquisición no ha sido fructífera, debido a que la solicitud de las licencias al proveedor fue con un corto plazo y no cuenta con las licencias, para proveer a la institución.

Recomendación

Que se cree una política de renovación de activos tecnológico, para que los mismos sean gestionados oportunamente y se garantiza la continuidad de los servicios que brinda la institución a la población Guatemalteca en general.

5. DETALLES DE FUNCIONARIOS Y PERSONAL RESPONSABLE

CARGO	NOMBRE	PERÍODO
Secretario de Junta Directiva	Lic. Edgar Alfredo Perez Prado	01/01/2014
Subgerente Administrativo	Lic. Sergio Alvarado Porras Torres	30/06/2014
Jefe del Departamento de informática	Ing. Diego Antonio Pérez Méndez	01/12/2013

CONCLUSIONES

1. La auditoría de tecnologías de información realizada en las entidades de gobierno, permitirá mejorar la funcionalidad de los diferentes componentes que conforman el gobierno de tecnologías de información en dichas entidades, de esta manera se obtendrá un nivel de confiabilidad y seguridad de la gestión de los activos tecnológicos; así como, de la información que se generan en pro del mejoramiento del bien común de la población.
2. Las normas gubernamentales actualmente carecen de una visión adecuada, en cuanto a la realización de una auditoría evaluando el gobierno de tecnologías de la información, por lo que la inexistencia de dicha normativa que rija el accionar del auditor interno, causa la falta de empoderamiento de la carrera de contaduría pública y auditoría de este tipo de auditoría.
3. La falta de políticas, estándares y objetivos que sean alineados con las nuevas tendencias en tecnología, pondrán de manifiesto, pobres gobiernos de tecnologías de la información, en entidades públicas, mismas que debería ser las primeras en adoptar, nuevos estándares que les permitan salvaguardar el erario público y el bien común de la población.
4. Los usuarios del sector público se benefician al recibir servicios de calidad respaldados por procesos, gente competente y estrategias basadas en un buen Gobierno de Tecnologías de la Información, alineado con mejores prácticas internacionales.

RECOMENDACIONES

1. Que los estudiantes de la facultad de ciencias económicas, profesionales y usuarios en general, interesados en fortalecer sus competencias de tecnologías de información, incorporen en su visión de formación los principios de Gobierno de Tecnologías de Información para fortalecer la gestión de las instituciones públicas y privadas en su esfuerzo por alcanzar objetivos.
2. Las instituciones que prestan servicios de salud deben incorporar buenas prácticas de gestión de Tecnologías de Información, con el objetivo de disminuir sus riesgos reputacionales y estratégicos, y así permitan asegurar que sus operaciones, estructuras y personal se desempeñan en pro del afiliado.
3. Se recomienda a las entidades de gobierno que establezcan políticas y controles para gestionar de una manera adecuada, de forma eficiente y eficaz la utilización de las tecnologías de información que son utilizadas en dicha entidad.
4. Incorporar las mejores prácticas de gestión de Tecnología de Información en conjunto con la emisión de normativa nacional para adoptar modelos de madurez de Gobierno de Tecnologías de Información y prestar mejores servicios en las entidades públicas de salud.

REFERENCIAS BIBLIOGRÁFICAS

1. Asamblea Nacional Constituyente. Constitución Política de la República de Guatemala. Guatemala, Guatemala: Diario oficial, 1985. pág. 77.

2. Comisión Guatemalteca de Normas del Ministerio de Economía, "Norma Técnica Guatemalteca, COGUANOR NTG/UNIT/ISO/IEC 27001:2005. pág. 49

3. Comisión Guatemalteca de Normas del Ministerio de Economía, "Norma Técnica Guatemalteca, COGUANOR NTG/UNIT/ISO/IEC 27002:2005. pág.167

4. Comisión Guatemalteca de Normas del Ministerio de Economía, "Norma Técnica Guatemalteca, COGUANOR NTG/UNIT/ISO/IEC 27005:2005. pág. 85

5. Comité Patrocinador de Organizaciones -COSO-. Los Nuevos Conceptos del Control Interno (Informe COSO). [ed.] 3a Juan Bravo. [trad.] S.A. Instituto Auditores Internos de España - Coopers & Lybrand. New York, Estados Unidos: Ediciones Díaz de Santos, S.A., 1992. pág. 420.

6. Congreso de la República de Guatemala. 31-2002 "Ley Orgánica de la Contraloría General de Cuentas, Diario Oficial, 2005, pág.75.

7. Congreso de la República de Guatemala. Decreto-Ley Número 106: "Código Civil", Diario Oficial, 1973. pág. 6.

8. Congreso de la República de Guatemala. Decreto-Ley Número 101-97 "Ley Orgánica del Presupuesto", Guatemala: Diario Oficial, 1997. pág. 79.

9. Contraloría General de Cuentas. Normas de Auditoría Gubernamental (Externa e Interna), 2006. pág 18.

10. Organización para la Cooperación y el Desarrollo Económicos -OCDE-. Principios de Gobierno Corporativo de la OCDE. [trad.] OCDE Publications. París, Francia: OECD 2004, 2004. pág. 68.

11. ISACA. COBIT 5. Rolling Meadows, Estados Unidos: ISACA, 2012. pág. 94. ISBN 978-1-60420-282-3.

12. Muñoz Razo, Carlos. Auditoría en Sistemas Computacionales. México:Pearson Educación, 2002. pág. 816. ISBN: 970-17-0405-3.

13. Oz, Effy. Administración de los sistemas de Información. [trad.] Miguel Ángel Martinez Sarmiento. Boston, Estados Unidos: Paraninfo, 2008. pág. 560. ISBN: 9789706867766.

14. Piattini, Mario, Del Peso, Emilio y Del Peso, Mar. Auditoría de Tecnologías y Sistemas de Información. México: Alfaomega Grupo Editor, S.A., 2008. pág. 732. ISBN: 978-970-15-1378-1.

WEB GRAFÍA

15. ISACA. La Historia de ISACA. [En línea] ISACA. [Citado el: 10 de febrero de 2016.] http://www.isaca.org/about-isaca/history/espanol/pages/default.aspx.

16. IIA. Normas internacionales para el ejercicio de la auditoría interna. [En línea] 2013. [Citado el: 10 de febrero de 2016.] http://www.iia.org/niepai2013.pdf.

17. ISO. Gobierno corporativo de las tecnologías de la información. [En línea] 2008. [Citado el: 10 de febrero de 2016.] http://www.iso.org/iso38500:2008