ANEXO 1. ANALISIS MARCO TEORICO

Nro.	Temática de TI	Descripción de la temática	ISO 38500	COBIT	PMBOK	ITIL	ISO 27001
1	**Documentos**	Documentos de referencia tomados como base para el análisis.	NTC-ISO/IEC 38500. (2009). NTC-ISO/IEC 38500: GOBIERNO CORPORATIVO DE LA TECNOLOGÍA	COBIT 5.ISACA. (2012). COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa	PMBOK-Project Management Institute. (2013). GUÍA DE LOS FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS - 5 Edición	ITIL- Office of Government Commerce. (2007). ITIL: The official introduction to the ITIL service lifecycle. TCM. (2012). Fundamentos de ITIL© Versión 3 Edición. ITIL Foundation. ITIL - Office of Government Commerce. (2007). ITIL: ITIL 3 Service Strategy	NTC-ISO/IEC 27001. (2006). NTC-ISO/IEC 27001: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información
2	**Propósito de la práctica**	Objetivo principal de la práctica	- Proporcionar un marco de principios para que los Directores los utilicen al evaluar, dirigir y monitorear el uso de la tecnología de la información (TI) en sus organizaciones (Pág. 6) - Guiar e informar a aquellos involucrados en el diseño y la implementación del sistema de gestión sobre políticas, procesos y estructuras que dan soporte al gobierno. (Pág. 6) - Esta norma proporciona principios de guía para los directores de las organizaciones (incluyendo, dueños, miembros de la junta, directores, socios, altos ejecutivos o similares) sobre el uso eficaz, eficiente y aceptable de la tecnología de la información (TI) en sus organizaciones. (Pág. 7) - El propósito de esta norma es fomentar el uso eficaz, eficiente y aceptable de la Tecnología de la Información en todas las organizaciones a través de las siguientes acciones: 1. Asegurar a las partes involucradas (incluyendo consumidores, accionistas y empleados) que, si se cumple la norma, pueden confiar en el Gobierno Corporativo que tiene la organización sobre la TI. 2. Informar y orientar a los directores sobre el gobierno del uso de la Tecnología de la Información en sus organizaciones. 3. Brindar una base para la evaluación objetiva del Gobierno Corporativo de la Tecnología de la Información. (Pág. 8) - Esta norma establece los principios para el uso eficaz, eficiente y aceptable de la Tecnología de la Información. El asegurar que sus organizaciones siguen estos principios facilitará a los directores equilibrar los riesgos y promover las oportunidades que se originan en el uso de la Tecnología de la Información. (Pág. 8)	- Provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde IT manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público. (Pág.. 13)	La Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK® Quinta Edición) proporciona pautas para la dirección de proyectos individuales y define conceptos relacionados con la dirección de proyectos. Describe asimismo el ciclo de vida de la dirección de proyectos y los procesos relacionados, así como el ciclo de vida del proyecto. La Guía del PMBOK® contiene el estándar, reconocido a nivel global y la guía para la profesión de la dirección de proyectos. Por estándar se entiende un documento formal que describe normas, métodos, procesos y prácticas establecidos. Al igual que en otras profesiones, el conocimiento contenido en este estándar evolucionó a partir de las buenas prácticas reconocidas de los profesionales dedicados a la dirección de proyectos que han contribuido a su desarrollo. (Pág.. 28)	La biblioteca de infraestructuras de tecnologías de la información (ITIL-Information Technology Infrastructure Library) proporciona un planteamiento sistemático para la provisión de servicios de TI con calidad mediante una serie de procesos y funciones integrados para entregar con alta calidad la provisión y el soporte de los servicios de TI. ITIL es un conjunto de buenas prácticas para la gestión de servicios de tecnologías de la información que suele enmarcarse en el ámbito del denominado gobierno de tecnologías de la información (IT Governance). (Pág. 9)	- Esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI). (Pág. 7) - Esta norma cubre todo tipo de organizaciones. Esta norma especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejora un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización.
3	**Gobierno y gestión**	Pautas y/o prácticas para el gobierno y la gestión de temáticas relacionadas con las tecnologías y la información.	- Esta norma brinda un marco para el gobierno eficaz de la Tecnología de la Información con el fin de ayudar a aquellos en los niveles más altos de las organizaciones a comprender y cumplir sus obligaciones legales, reglamentarias y éticas con respecto al uso que le dan sus organizaciones a la Tecnología de la Información. Este marco abarca definiciones, principios y un modelo. (Pág. 6) - El gobierno es diferente de la gestión. (Pág. 6) PRINCIPIO 3: ADQUISICIÓN (Pág.16) 1. Evaluar Los directores deberían evaluar las opciones para el suministro de la Tecnología de la información con el fin de realizar las propuestas aprobadas, equilibrando los riesgos y el valor del dinero de las inversiones propuestas 2. Dirigir Los directores deberían gestionar que los activos de Tecnología de la información (sistemas e infraestructura) se adquieran de la manera correcta, incluida la preparación de la documentación adecuada, a la vez que se asegura el suministro de las capacidades requeridas. Los directores deberían gestionar que los acuerdos de suministro (tanto interno como externo) den soporte a las necesidades del negocio de la organización. 3. Monitorear Los directores deberían monitorear las inversiones en Tecnología de la información para asegurar que éstas proporcionan las capacidades requeridas. Se recomienda que los directores monitoreen el grado en el que su organización y sus proveedores mantienen el entendimiento compartido de la intención de la organización al hacer cualquier adquisición de Tecnología de la información PRINCIPIO 5: CONFORMIDAD (Pág. 18) Monitorear Es recomendable que los directores monitoreen la conformidad y el cumplimiento de la Tecnología	- Principio 2: Cubrir la Empresa Extremo-a-Extremo—COBIT integra el gobierno y la gestión de TI en el gobierno corporativo: – Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos – internos y externos – los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.(Pág.. 14) - Principio 3: Aplicar un Marco de Referencia único integrado—Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa. (Pág.. 14) - Principio 5: Separar el Gobierno de la Gestión— El marco de trabajo COBIT establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. La visión de COBIT en esta distinción clave entre gobierno y gestión es: 1. Gobierno: El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a	Presenta prácticas en gobierno y gestión de proyectos. Dentro de sus prácticas de gobierno está la PMO (Oficina de dirección de proyectos). Una oficina de dirección de proyectos (PMO) es una estructura de gestión que estandariza los procesos de gobierno relacionados con el proyecto y hace más fácil compartir recursos, metodologías, herramientas y técnicas. Las responsabilidades de una PMO pueden abarcar desde el suministro de funciones de soporte para la dirección de proyectos hasta la responsabilidad de la propia dirección de uno o más proyectos. (Pág.. 38) Existen diferentes tipos de estructuras de PMOs en las organizaciones, en función del grado de control e influencia que ejercen sobre los proyectos en el ámbito de la organización. Por ejemplo: • De apoyo. Las PMOs de apoyo desempeñan un rol consultivo para los proyectos, suministrando plantillas, mejores prácticas, capacitación, acceso a la información y lecciones aprendidas de otros proyectos. Este tipo de PMO sirve como un repositorio de proyectos. Esta PMO ejerce un grado de control reducido. • De control. Las PMOs de control proporcionan soporte y exigen cumplimiento por diferentes medios. Este cumplimiento puede implicar la adopción de marcos o metodologías de dirección de proyectos a través de plantillas, formularios y herramientas específicos, o conformidad en términos de gobierno. Esta PMO ejerce un grado de control moderado. • Directiva. Las PMOs directivas ejercen el control de los proyectos asumiendo la propia dirección de los mismos. Estas PMOs ejercen un grado de control elevado. (Pág.. 38)	Gobierno de TI son los procesos, procedimientos y estructura organizacional que realiza el área de TI en coordinación con la alta dirección para gestionar y controlar las actividades que buscan alcanzar los objetivos del área y del negocio. ITIL es una forma de gestionar y controlar los servicios de TI. En general el gobierno de TI: - Busca asegurar que la estrategia de TI está alineada con el negocio. - Dar a la organización el mayor valor posible y de la forma más eficiente las funciones y servicios de TI. - Mitigar los riesgos y asegurar los recursos de TI. - Asegurar el cumplimiento de las normas y regulaciones en forma general y de los marcos de referencia o estándares para llegar a cumplirlas. (Pág. 18)	- Para el establecimiento de SGSI la organización debe: 1. Definir un alcance y límites de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos, tecnología, e incluir los detalles y justificación de cualquier exclusión del alcance. 2. Definir una política de SGSI en términos de las características del negocio, la organización, su ubicación, sus activos y tecnología, que: - Incluya un marco de referencia para fijar objetivos y establezca un sentido general de dirección y principios para la acción con relación a la seguridad; - Tenga en cuenta los requisitos del negocio, los legales o reglamentarios, y las obligaciones de seguridad contractuales; - Esté alineada con el contexto organizacional estratégico de gestión del riesgo en el cual tendrá lugar el establecimiento y mantenimiento del SGSI. - Establezca los criterios contra los cuales se evaluará el riesgo (Pág. 13) - Haya sido aprobada por la dirección. (Pág. 14) - Para la implementación y operación del SGSI la organización debe: 1. Formular un plan para el tratamiento de riesgos que identifique la acción de gestión apropiada, los recursos, responsabilidades y prioridades para manejar los riesgos de seguridad de la información 2. Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluya considerar la financiación y la asignación de funciones y responsabilidades 3. Implementar programas de formación y de toma de conciencia 4. Gestionar la operación del SGSI 5. Gestionar los recursos del SGSI
4	**Arquitectura empresarial**	Pautas y/o prácticas para la definición y alineación de la arquitectura de TI con la arquitectura empresarial.	No presenta relación con la temática	- COBIT es un marco de referencia único e integrado porque: • Se alinea con otros estándares y marcos de referencia relevantes y, por tanto, permite a la empresa usar COBIT 5 como el marco integrador general de gestión y gobierno. • Es completo en cuanto a la cobertura de la empresa, proporcionando una base para integrar de manera efectiva otros marcos, estándares y prácticas utilizadas. Un marco general único sirve como una fuente consistente e integrada de guía en un lenguaje común, no-técnico y tecnológicamente agnóstico. • Proporciona una arquitectura simple para estructurar los materiales de guía y producir un conjunto consistente. - El marco de referencia COBIT 5 proporciona a sus grupos de interés la guía más completa y actualizada (ver figura 11) sobre el gobierno y la gestión de la empresa TI mediante: La investigación y utilización de un conjunto de fuentes que han impulsado el nuevo contenido desarrollado, incluyendo: - La unión de todas las guías existentes de ISACA (COBIT4.1, Val IT 2.0, Risk IT, BMIS) en este único marco. – Completar este contenido con áreas que necesitaban más elaboración y actualización. – El alineamiento a otros estándares y marcos relevantes, tales como ITIL, TOGAF y estándares ISO (Pág.. 26)	No presenta relación con la temática.	La arquitectura empresarial que según The Open Group Architecture (TOGAF) incluye: la arquitectura de procesos, arquitectura de información, arquitectura de aplicaciones y arquitectura tecnológica, son entradas importantes para cada una de las etapas del ciclo de vida del servicio. En cada etapa del ciclo de vida se tienen en cuenta los elementos relacionados con la arquitectura que se desprenden de la estrategia de negocio y la estrategia de TI. ITIL tiene una relación estrecha con el marco The Open Group Architecture (TOGAF) debido a que se deben tener en cuenta las prácticas y definiciones de arquitectura empresarial para asegurar la alineación y calidad los servicios de TI.	No presenta relación con la temática.
5	**Generación de valor**	Pautas y/o prácticas para la generación de valor y medición de los beneficios en tecnologías de la información.	No presenta relación con la temática	- Principio 1. Satisfacer las Necesidades de las Partes Interesadas: Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos. COBIT provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos. (Pág.. 14)	- El valor del negocio es un concepto único para cada organización. El valor del negocio se define como el valor del negocio en su totalidad, como la suma total de sus elementos tangibles e intangibles. Como ejemplos de elementos tangibles se pueden citar los activos monetarios, los equipos, la participación de los accionistas y los servicios. Como ejemplos de elementos intangibles se pueden citar la buena voluntad, el reconocimiento de marca, el beneficio público y las marcas registradas. Dependiendo de la organización, el alcance del valor del negocio puede ser a corto, mediano o largo plazo. Se puede crear valor a través de la gestión eficaz de las operaciones permanentes. No obstante, a través del uso eficaz de la dirección de portafolios, la dirección de programas y la dirección de proyectos, las organizaciones tendrán la capacidad de emplear procesos establecidos y confiables para cumplir con los objetivos estratégicos y obtener mayor valor de negocio a partir de sus inversiones en proyectos. Si bien no todas las organizaciones están orientadas al negocio, todas ellas desarrollan actividades relacionadas con el negocio. Ya sea que se trate de una agencia gubernamental o de una organización sin fines de lucro, todas las organizaciones se centran en lograr valor de negocio para sus actividades. (Pág.. 42) - Mediante la dirección de proyectos las organizaciones pueden aplicar el conocimiento, los procesos, las habilidades y las herramientas y técnicas para incrementar la probabilidad de éxito en un gran número de proyectos. La dirección de proyectos se centra en la entrega satisfactoria de productos, servicios o resultados. En el ámbito de programas y portafolios, los proyectos constituyen un medio para lograr los objetivos y la estrategia organizacional. (Pág. 43)	En cada etapa del ciclo de vida del servicio se proporciona valor al negocio. En todas las etapas hay procesos distintos, funciones y actividades que trabajar juntos para alcanzar los objetivos de servicio. (10) Los servicios son definidos en ITIL como un medio de aportar valor al cliente sin que éste deba asumir los riesgos y costos específicos de su prestación. Pero el valor al que nos referimos no depende exclusivamente del valor económico asociado al resultado específico de cada servicio. La forma de generar valor es asegurarle al cliente es que el servicio tenga la "utilidad" requerida y que se preste con la "garantía" acordada. Desde el punto de vista positivo, la utilidad ofrecida que debe adaptarse a las necesidades reales del cliente, la garantía del proveedor que asegura que el servicio se prestará de forma continuada preservando los niveles de calidad acordados. Desde el punto de vista negativo, se puede tener la pérdida de control de todo el proceso, costos ocultos, una inferior calidad, "caer cautivo" en manos de un proveedor de servicios. El proveedor debe tener en cuenta que el valor para el cliente está en el resultado del servicio y el impacto que éste tiene en su negocio y no en el servicio en sí mismo. La utilidad y garantía de un servicio son con frecuencia interdependientes y a la hora de concebir un nuevo servicio la organización TI debe buscar un equilibrio entre ambas minimizando a su vez los aspectos que los potenciales clientes puedan percibir	No presenta relación con la temática.
6	**Alineación con la estrategia empresarial**	Pautas y/o prácticas para la alineación de la estratega de la TI con la estrategia y objetivos de la empresa.	- El Gobierno Corporativo adecuado de la Tecnología de la Información ayuda a los directores a garantizar que el uso de la Tecnología de la Información contribuye de manera positiva al desempeño de la organización a través de: 1. la implementación y operación adecuadas de los activos de la Tecnología de la Información; 2. claridad de la responsabilidad, acciones y decisiones tanto para el uso como la provisión de la tecnología de la información en el logro de las metas de la organización; 3. continuidad y sostenibilidad del negocio; 4. alineación de la Tecnología de la Información con las necesidades del negocio; 5. asignación eficiente de los recursos; 6. innovación en los servicios, los mercados y los negocios; 7. buenas prácticas en las relaciones con las partes involucradas; 8. reducción en los costos para la organización y 9 Comprensión real de los beneficios buscados a partir de cada inversión en Tecnología de la Información. (Pág. 9) - Los directores deberían controlar la Tecnología de la Información a través de tres tareas principales: 1. Evaluar el uso actual y futuro de la Tecnología de la Información. 2. Dirigir la preparación e implementación de los planes y las políticas para garantizar que el uso de la TI satisface los objetivos del negocio. 3. Monitorear la conformidad con las políticas y el desempeño frente a los planes (Pág. 13) Ver grafica: Figura 1. Modelo para el Gobierno Corporativo de la TI - Evaluar: Los directores deberían examinar y juzgar el uso corriente y futuro de la Tecnología de la Información, considerando estrategias, propuestas y acuerdos de terceros (para terceros externos	- Principio 4: Hacer Posible un Enfoque Holístico—Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT define siete categorías de catalizadores: – Principios, Políticas y Marcos de Trabajo – Procesos – Estructuras Organizativas – Cultura, Ética y Comportamiento – Información – Servicios, Infraestructuras y Aplicaciones – Personas, Habilidades y Competencias (Pág.. 14) - Las necesidades de las partes interesadas deben transformarse en una estrategia corporativa factible. La cascada de metas de COBIT es el mecanismo para traducir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida. Esta traducción permite establecer metas específicas en todos los niveles y en todas las áreas de la empresa en apoyo de los objetivos generales y requisitos de las partes interesadas y así	1. Vínculo entre la Dirección de Proyectos y el Gobierno Corporativo: Los proyectos (y los programas) se emprenden con el fin de alcanzar resultados estratégicos para el negocio, para lo que numerosas organizaciones están adoptando actualmente procesos y procedimientos formales de gobierno corporativo. Los criterios de gobernabilidad de la organización pueden imponer restricciones a los proyectos —en especial si el proyecto entrega un servicio sujeto a un gobierno corporativo estricto. (Pág.. 42) 2. Vínculo entre la Dirección de Proyectos y la Estrategia Organizacional: La estrategia organizacional debe proporcionar guía y dirección a la dirección de proyectos—especialmente si se tiene en cuenta que los proyectos existen para sustentar la estrategia organizacional. A menudo es el patrocinador del proyecto o el director del programa o portafolio quién identifica el alineamiento o los potenciales conflictos entre estrategias organizacionales y objetivos del proyecto y lo comunica al director del proyecto. Cuando los objetivos del proyecto entran en conflicto con la estrategia organizacional establecida, es responsabilidad del director del proyecto identificar y documentar cuanto antes dichos conflictos. En ocasiones, el desarrollo de una estrategia organizacional puede constituir el objetivo de un proyecto, en lugar de un principio rector. Si este es el caso, es importante que el proyecto defina especificamente los términos de una estrategia organizacional adecuada que sustente la organización. (Pág.. 42)	La arquitectura de procesos, arquitectura de información, arquitectura de aplicaciones y arquitectura tecnológica, son elementos importantes para cada una de las etapas del ciclo de vida del servicio. En cada etapa del ciclo de vida se tienen en cuenta los elementos relacionados con la arquitectura que se desprende de la estrategia de negocio y la estrategia de TI. La fase de "Estrategia del servicio" proporciona una guía acerca de como utilizar la gestión de servicios de TI como una herramienta clave para satisfacer las necesidades del negocio y para apoyar el logro de la estrategia empresarial. En esta fase: - Se proporciona una guía de como implementar la gestión del servicio como una herramienta estratégica. - Se recibe la perspectiva, planes y lineamientos de la estrategia del negocio. - Establece los principios para desarrollar las políticas de las gestión del servicio, directrices y procesos a lo largo del ciclo de vida del servicio. - Identifica y prioriza las oportunidades. - Asegura que las organizaciones puedan manejar los costos y riesgos asociados con su portafolio de servicios.	- en la provisión de recursos la organización debe determinar y suministrar los recursos necesarios para: Asegurar que los procedimientos de seguridad de la información brindan apoyo a los requisitos del negocio Identificar y atender los requisitos leales y reglamentarios, así como las obligaciones de seguridad contractuales Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados (Pág. 20)
7	**Procesos y prácticas**	Procesos, pautas y/o prácticas para el gobierno y gestión de las temáticas relacionadas con las tecnologías y la información.	- Principios: Esta sección establece seis principios para el buen Gobierno Corporativo de la Tecnología de la Información. Los principios se aplican a la mayoría de las organizaciones. Los principios expresan el comportamiento de preferencia para guiar la toma de decisiones. La declaración de cada principio se refiere a lo que debería suceder, pero no prescribe cómo, cuándo o por parte de quién se implementarán los principios - dado que estos aspectos dependen de la naturaleza de la organización que implementa los principios. Es recomendable que los directores exijan que se apliquen estos principios. (Pág. 12) 1. Principio: Responsabilidad Los individuos o grupos dentro de la organización entienden y aceptan sus responsabilidades con respecto tanto al suministro como a la demanda de Tecnología de la Información. Aquellos con responsabilidad de las acciones también tienen la autoridad para ejecutar tales acciones. 2. Principio: Estrategia La estrategia de negocios de la organización toma en consideración las capacidades actuales y futuras de la Tecnología de la Información; los planes estratégicos para la Tecnología de la Información satisfacen las necesidades actuales y continuas de la estrategia de negocios de la organización 3. Principio: Adquisición Las adquisiciones de Tecnología de la Información se hacen por razones válidas, con base en el análisis adecuado y continuo, con toma de decisiones clara y transparente. Existe el equilibrio adecuado entre beneficios, oportunidades, costos y riesgos, tanto a corto como a largo plazo. 4. Principio: Desempeño La Tecnología de la Información es adecuada para brindar soporte a la organización, suministrando los servicios, los niveles de servicio y la calidad del servicio que se requieren para satisfacer los requisitos actuales y futuros del negocio 5. Principio: Conformidad	- Principio 2: Cubrir la Empresa Extremo-a-Extremo—COBIT integra el gobierno y la gestión de TI en el gobierno corporativo: – Cubre todas las funciones y procesos dentro de la empresa; COBIT no se enfoca sólo en la "función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.(Pág.. 14) - Catalizador: Los procesos describen un conjunto organizado de prácticas y actividades para alcanzar ciertos objetivos y producir un conjunto de resultados que soporten las metas generales relacionadas con TI. (Pág. 27)	- La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo. Esta aplicación de conocimientos requiere de la gestión eficaz de los procesos de dirección de proyectos. (Pág.. 74) - La Guía del PMBOK® describe exclusivamente los procesos de la dirección de proyectos. Si bien los procesos orientados al producto están fuera del alcance de este documento, el director del proyecto y el equipo del proyecto no debieran ignorarlos. Los procesos de la dirección de proyectos y los procesos orientados al producto se superponen y actúan los unos sobre los otros a lo largo de la vida de un proyecto. (Pág.. 75) - La Guía del PMBOK® describe la naturaleza de los procesos de la dirección de proyectos en términos de la integración entre los procesos, de sus interacciones y de los propósitos a los que responden. Los procesos de la dirección de proyectos se agrupan en cinco categorías conocidas como Grupos de Procesos de la Dirección de Proyectos (o Grupos de Procesos). (Pág.. 75) • Grupo de Procesos de Inicio. Aquellos procesos realizados para definir un nuevo proyecto o nueva fase de un proyecto existente al obtener la autorización para iniciar el proyecto o fase. • Grupo de Procesos de Planificación. Aquellos procesos requeridos para establecer el alcance del proyecto, refinar los objetivos y definir el curso de acción requerido para alcanzar los objetivos propuestos del proyecto. • Grupo de Procesos de Ejecución. Aquellos procesos realizados para completar el trabajo definido en el plan para la dirección del proyecto a fin de satisfacer las especificaciones del mismo. • Grupo de Procesos de Monitoreo y Control. Aquellos procesos requeridos para rastrear,	La gestión del servicio es un conjunto de capacidades y especializaciones organizacionales dedicadas a generar valor a los clientes en forma de servicios, esas capacidades se refieren a funciones, procesos y roles para administrar el ciclo de vida del servicio (Estrategia, Diseño, Transición, Operación y Mejora continua). - Estrategia: Proporciona una guía de cómo utilizar la gestión de servicios como una herramienta estratégica para satisfacer las necesidades del negocio. - Diseño: Proporciona una guía para el diseño de servicios (nuevos o modificados) y para los procesos de gestión de servicios. - Transición: Proporciona una guía para una transición a la operación de nuevos servicios y los que están cambiando sin complicaciones. - Operación: Proporciona una guía para lograr una entrega efectiva y eficaz, y soporte de los servicios para asegurar el valor para el cliente y el proveedor de servicios. - Mejora continua: Proporciona una guía para ayudar a mantener y mejorar el diseño , transición y operación de los servicios alineados a los requerimientos cambiantes del del negocio. La gestión del servicio se compone de cuatro (4) elementos fundamentales: - Personas: Cumplen funciones en la organización y roles en los procesos. - Productos: Representan los elementos de la infraestructura. - Procesos: Organizan la gestión de los productos. - Proveedores: Apoyan a las organizaciones dentro de los procesos y en la gestión de los productos.	- Esta norma promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento. Mantener y mejorar el SGSI de una organización. Para funcionar eficazmente, una organización debe identificar y gestionar muchas actividades. Se puede considerar como un proceso cualquier actividad que use recursos y cuya gestión permita la transformación de entradas y salidas. Con frecuencia, el resultado de un proceso constituye directamente la entrada del proceso siguiente. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones entre estos procesos, y su gestión, se puede denominar como un "enfoque basado en procesos" (Pág. 7) - Esta norma adopta el modelo de procesos "planificar - hacer - verificar – actuar" (PHVA), que se aplica para estructurar todos los procesos del SGSI. (Pág. 8) - La organización debe mejorar continuamente la eficacia del SGSI mediante el uso de la política de seguridad de la información, los objetivos de seguridad de la información, los resultados de la auditoría, el análisis de los eventos a los que se les ha hecho seguimiento, las acciones correctivas y preventivas y la revisión por la dirección. (Pág. 23)

ANEXO 1. ANALISIS MARCO TEORICO

Nro.	Temática de TI	Descripción de la temática	ISO 38500	COBIT	PMBOK	ITIL	ISO 27001
8	**Roles y responsabilidades**	Pautas y/o prácticas para la definición de la estructura formal para el gobierno y gestión de las tecnologías y la información.	- Aunque esta norma esta dirigida principalmente al organismo de gobierno, que a su vez puede requerir que la gerencia de la organización emprenda algunas acciones, también permite que, en algunas organizaciones (por lo general más pequeñas), los miembros del organismo de gobierno ocupen los roles claves en la gerencia. De esta manera garantiza que la norma sea aplicable a todas las organizaciones, desde la más pequeña hasta la más grande, independientemente del propósito, el diseño y la estructura de propiedad. (Pág. 6) - Para el propósito de esta norma, se aplican las definiciones que se indican a continuación. Se espera que una organización adapte la terminología utilizada en esta norma a sus circunstancias o su estructura. (Pág. 9) 1. Gobierno corporativo: Sistema mediante el cual se dirigen y controlan las organizaciones. (Adaptado de Cadbury 1992 y OECD 1999). 2. Gobierno corporativo de TI: Sistema mediante el cual se dirige y controla el uso actual y futuro de la Tecnología de la Información. El Gobierno Corporativo de la TI implica la evaluación y dirección del uso de dicha tecnología para dar soporte a la organización y el monitoreo de este uso para alcanzar los planes. Éste incluye la estrategia y las políticas para utilizar la Tecnología de la Información dentro de una organización. 3. Director: Miembro del organismo de gobierno más alto de una organización. Se incluyen dueños, miembros de la junta, socios, ejecutivos de alto nivel o similares y funcionarios autorizados por la legislación o los reglamentos 4. Tecnología de la información: Recursos que se requieren para adquirir, procesar, almacenar y divulgar la información. Este término también incluye "tecnología de la comunicación (TC)" y el término combinado "tecnología de la información y la comunicación (TIC)". (Pág. 10) 5. Parte involucrada: Todo individuo, grupo u organización que puede afectar, verse afectado o percibirse a sí mismo como afectado por una decisión o una actividad (adaptado de Guía ISO/IEC 73). (Pág. 11)	- Gobierno: En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas. - Gestión: En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director General Ejecutivo (CEO). (Pág.. 14). - Las personas, habilidades y competencias están relacionadas con las personas y son necesarias para poder completar de manera satisfactoria todas las actividades y para la correcta toma de decisiones y de acciones correctivas. (Pág. 27)	- La gobernabilidad del proyecto es una función de supervisión que está alineada con el modelo de gobierno de la organización y que abarca el ciclo de vida del proyecto. El marco de gobernabilidad del proyecto proporciona al director y al equipo del proyecto la estructura, los procesos, los modelos de toma de decisiones y las herramientas para dirigir el proyecto, a la vez que apoya y controla el proyecto para lograr una entrega exitosa. La gobernabilidad del proyecto es un elemento crítico de cualquier proyecto, particularmente en el caso de proyectos complejos y de alto riesgo. Proporciona un método integral y coherente para controlar el proyecto y asegurar el éxito mediante la definición, documentación y comunicación de prácticas de proyecto fiables y repetibles. Incluye un marco para la toma de decisiones en el proyecto, define roles y responsabilidades, medidas para definir el éxito del mismo y determinar la eficacia del director del proyecto. La gobernabilidad de un proyecto se define y se integra en el contexto más amplio del portafolio, programa u organización que lo patrocina, pero es ajena al gobierno de la organización. (Pág.. 61) - El equipo del proyecto incluye al director del proyecto y al grupo de individuos que actúan conjuntamente en la realización del trabajo del proyecto para alcanzar sus objetivos. El equipo del proyecto incluye al director del proyecto, al personal de dirección del proyecto y a otros miembros del equipo que desarrollan el trabajo, pero que no necesariamente participan en la dirección del proyecto. Este equipo está compuesto por individuos procedentes de diferentes grupos, con conocimientos en una materia específica o con un conjunto de habilidades específicas para llevar a cabo el trabajo del proyecto. La estructura y las características de un equipo de proyecto pueden variar ampliamente, pero una constante es el rol del director del proyecto como líder del equipo, independientemente de la autoridad que éste pueda tener sobre sus miembros. (Pág.. 62)	Al diseñar un servicio o proceso es necesario definir claramente todos los roles, para permitir la toma de decisiones rápida y efectiva. ITIL establece unos roles y funciones, y utiliza el modelo RACI (Responsable, Accountable, Consulted and Informed) para administrar mejor los procesos y definir adecuadamente los roles y las responsabilidades. Establece los siguientes roles y funciones: - Función: Unidad organizacional especializada en la ejecución de actividades específicas y responsable de la entrega de resultados. - Dueño del proceso: Responsable de ejecutar que el proceso es ejecutado efectivamente, eficientemente, cumple con los requerimientos y realiza la mejora continua. - Dueño del servicio: Responsable de un servicio específico y lo representa en toda la organización. - Cliente: Alguien que compra bienes o servicios. - Usuario: Persona que utiliza el servicio de TI en el día a día.	- La dirección debe brindar evidencia del su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora del SGSI: Mediante el establecimiento de una política del SGSI Asegurando que se establezcan los objetivos y planes del SGSI Estableciendo funciones y responsabilidades de seguridad de la información (Pág. 20) Comunicando a la organización la importancia de cumplir los objetivos de seguridad de la información y de la conformidad con la política de seguridad de la información, sus responsabilidades bajo la ley, y la necesidad de la mejora continua Brindando los recursos suficientes para establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI Decidiendo los criterios para aceptación de riesgos, y los niveles de riesgo aceptables Asegurando que se realizan auditorías internas del SGSI Efectuando las revisiones por la dirección, del SGSI - Para la formación, toma de conciencia y competencia la organización debe asegurar que todo el personal al que se asigne responsabilidades definidas en el SGSI sea competente para realizar las tareas exigidas, mediante: 1. La determinación de las competencias necesarias para el personal que ejecute el trabajo que afecta el SGSI 2. El suministro de formación o realización de otras acciones para satisfacer las necesidades 3. La evaluación de la eficacia de las acciones emprendidas, y 4. El mantenimiento de registros de la educación, formación, habilidades, experiencia y calificaciones (Pág. 20)
9	**Seguridad de la información**	Pautas y/o prácticas para el manejo de la seguridad de la información en la empresa.	- Los directores aseguren que la transición de los proyectos al estado operativo se planifica y gestiona adecuadamente, tomando en consideración los impactos en el negocio y las prácticas operativas, así como también los sistemas y la infraestructura de TI ya existentes. (Pág. 14) PRINCIPIO 4: DESEMPEÑO (Pág. 17) Dirigir Los directores deberían asegurar la asignación de recursos suficientes de manera tal que la Tecnología de la información satisfaga las necesidades de la organización, de acuerdo con las prioridades acordadas y las restricciones del presupuesto. Los directores deberían dirigir a aquellos responsables de asegurar que la Tecnología de la información de soporte al negocio, cuando se requiera por razones del negocio, con datos correctos y actualizados que estén protegidos contra pérdida o mal uso	- COBIT 5 proporciona la guía de nueva generación de ISACA para el gobierno y la gestión de las TI en la empresa. Se construye sobre más de 15 años de uso práctico y aplicación de COBIT por parte de muchas empresas y usuarios de las comunidades de negocio, TI, riesgo, seguridad y aseguramiento. (Pág. 15) Integra los principales marcos y guías de ISACA, con un enfoque principal en COBIT, ValIT y RiskIT, pero considerando también el Modelo de Negocio para la Seguridad de la Información (BMIS), el Marco de Aseguramiento de TI (ITAF), la publicación titulada Board Briefing on IT Governance y el documento Taking Governance Forward (TGF), de modo que COBIT 5 cubra la actividad de la empresa al completo y proporcione una base para integrar otros marcos, normas y prácticas como un marco único. (Pág. 15)	No presenta relación con la temática.	"Seguridad de la información es una actividad de gestión dentro de la marco de gobierno corporativo, que proporciona la dirección estratégica para las actividades de seguridad y garantiza se logran los objetivos. Se asegura, además, que la que los riesgos de seguridad de información se gestionan de manera adecuada y los recursos de información de la empresa se utilizan de forma responsable. Dentro de las funciones y procesos asociados directamente a la fase de Diseño del Servicio y relacionados con la seguridad de la información se tiene: (11) - Gestión de la Seguridad de la Información: responsable de establecer las políticas de integridad, confidencialidad y disponibilidad de la información. La información es inherente al negocio y su correcta gestión debe apoyarse en tres pilares fundamentales: - Confidencialidad: la información debe ser sólo accesible a sus destinatarios predeterminados. - Integridad: la información debe ser correcta y completa. -Disponibilidad: debemos de tener acceso a la información cuando la necesitamos. La Gestión de la Seguridad debe, por tanto, velar por que la información sea correcta y completa, esté siempre a disposición del negocio y sea utilizada sólo por aquellos que tienen	- La adopción del modelo PHVA también reflejará los principios establecidos en las Directrices OCDE (2002) que controlan la seguridad de sistemas y redes de información. Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad. Directrices OCDE (2002) : para la seguridad de sistemas y redes de información. Hacia una cultura de la seguridad. - Esta norma especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas. - El SGSI está diseñado para asegurar controles de seguridad suficientes y proporcionales que protejan los activos de información y brinden confianza a las partes interesadas. (Pág. 10)
10	**Gestión de riesgos**	Pautas y/o prácticas para el manejo integral del ciclo de gestión de riesgos en temáticas relacionadas con las tecnologías y la información.	- Esta norma establece un modelo para el gobierno de la Tecnología de la Información. El riesgo de que los directores no cumplan sus obligaciones se reduce a prestar atención debida al modelo en la aplicación correcta de los principios. (Pág. 8) - Los sistemas de TI inadecuados pueden exponer a los directores al riesgo de no cumplir con las leyes. Por ejemplo, en algunas jurisdicciones, los directores pueden tener responsabilidad personal si un sistema contable inadecuado ocasiona el no pago de los impuestos. (Pág. 8) - Los procesos que tratan de la TI incorporan riesgos que se deben tratar adecuadamente. Por ejemplo, los directores podrían ser responsables debido a incumplimientos de: 1. normas de seguridad; 2. Legislación sobre privacidad; 3. legislación sobre correo masivo; 4. legislación sobre prácticas comerciales; 5. derechos de propiedad intelectual, incluyendo acuerdos sobre licencias de software; 6. requisitos de conservación de registros; 7. legislación y reglamentación ambiental; 8. legislación sobre salud y seguridad; 9. legislación sobre accesibilidad; 10. normas sobre responsabilidad social. nota: Es más probable que los directores que usan las directrices de esta norma cumplan con sus obligaciones. (Pág. 8) PRINCIPIO 4: DESEMPEÑO (Pág. 17) 1. Evaluar Los directores deberían evaluar los medios propuestos por los gerentes para asegurar que la Tecnología de la información apoye los procesos de negocio con la habilidad y capacidad	- Integra todo el conocimiento disperso previamente en los diferentes marcos de ISACA. ISACA ha investigado las áreas clave del gobierno corporativo durante muchos años y ha desarrollado marcos tales como COBIT, Val IT, Risk IT, BMIS, la publicación Información sobre Gobierno de TI para la Dirección (Board Briefing on IT Governance) e ITAF para proporcionar guía y asistencia a las empresas. COBIT 5 integra todo este conocimiento. (Pág. 25)	- La Gestión de los Riesgos del Proyecto incluye los procesos para llevar a cabo la planificación de la gestión de riesgos, así como la identificación, análisis, planificación de respuesta y control de los riesgos de un proyecto. Los objetivos de la gestión de los riesgos del proyecto consisten en aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos negativos en el proyecto. (Pág.. 336) • Planificar la Gestión de los Riesgos: El proceso de definir cómo realizar las actividades de gestión de riesgos de un proyecto. • Identificar los Riesgos: El proceso de determinar los riesgos que pueden afectar al proyecto y documentar sus características. • Realizar el Análisis Cualitativo de Riesgos: El proceso de priorizar riesgos para análisis o acción posterior, evaluando y combinando la probabilidad de ocurrencia e impacto de dichos riesgos. • Realizar el Análisis Cuantitativo de Riesgos: El proceso de analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto. • Planificar la Respuesta a los Riesgos: El proceso de desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. • Controlar los Riesgos: El proceso de implementar los planes de respuesta a los riesgos, dar seguimiento a los riesgos identificados, monitorear los riesgos residuales, identificar nuevos riesgos y evaluar la efectividad del proceso de gestión de los riesgos a través del proyecto. (Pág.. 336)	El punto de partida para la gestión de riesgos es la estrategia de continuidad del negocio y teniendo como base el análisis de impacto en el negocio (Business Impact Analysis - BIA). En la etapa de Diseño del Servicio se realiza el análisis de riesgos sobre los activos críticos para la empresa y se establece el nivel de riesgo al que están expuestos estos activos, la valoración del riesgo (cualitativo y cuantitativo) y la estrategia de continuidad de los servicios de TI.	- Definir el enfoque organizacional para la valoración del riesgo: 1. Identificar una metodología de valoración del riesgo que sea adecuada al SGSI y a los requisitos reglamentarios, legales y de seguridad de la información del negocio, identificados. 2. Desarrollar criterios para la aceptación de riesgos, e identificar los niveles de riesgo aceptables. La metodología seleccionada para la valoración de riesgos debe asegurar que dichas valoraciones producen resultados comparables y reproducibles. - Identificar los riesgos 1. identificar los activos dentro del alcance del SGSI y los propietarios de estos activos 2. Identificar las amenazas a estos activos 3. Identificar las vulnerabilidades que podrían ser aprovechadas por las amenazas 4. Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos - Analizar y evaluar el riesgo 1. Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos 2. Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente 3. Estimar los niveles de los riesgos 4. Determinar la aceptación del riesgo o la necesidad de su tratamiento - Identificar y evaluar las opciones para el tratamiento de los riesgos (Pág. 14)
11	**Toma de decisiones**	Pautas y/o prácticas para la definición de la estructura y niveles de aprobación usados en el gobierno y gestión de las tecnologías y la información.	Esta norma se aplica al gobierno de los procesos de gestión (y las decisiones) relacionados con los servicios de información y comunicación utilizados por la organización. Estos procesos podrían ser controlados por los especialistas en TI de la organización, por proveedores externos del servicio o por unidades de negocios dentro de la organización. También orienta a quienes asesoran, informan o asisten a los directores. Se incluyen: - altos directivos; - miembros de grupos que monitorean los recursos dentro de la organización; - especialistas externos técnicos o en negocios, tales como legales o contables; especialistas, asociaciones al detal u organismos profesionales; - distribuidores de software, hardware, comunicaciones y otros productos de TI; - proveedores internos y externos de servicios (incluyendo consultores); - auditores de TI. (Pág. 7)	- Catalizador: Las estructuras organizativas son las entidades de toma de decisiones clave en una organización. (Pág. 27)	- Estructura de Desglose de la Organización (OBS). Una representación jerárquica de la organización del proyecto que ilustra la relación entre las actividades del proyecto y las unidades de la organización que llevarán a cabo esas actividades. (Pág.. 570)	La toma de decisiones está directamente relacionada con los roles y responsabilidades establecidas en la matriz RACI.	- La dirección debe revisar el SGSI de la organización a intervalos planificados, para asegurar su conveniencia, suficiencia y eficacia continuas. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros. (Pág. 21)
12	**Comunicación con los interesados**	Pautas y/o prácticas para la socialización, divulgación y distribución de la información relacionada con temáticas relacionadas con las tecnologías y la información.	No presenta relación con la temática	- Catalizador: Cultura, ética y comportamiento se refiere al conjunto de conductas individuales y colectivas dentro de una empresa. (Pág. 79) El modelo de cultura, ética y comportamiento muestra: Buenas prácticas—Las 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. – Concienciación de los comportamientos deseados, fortalecidos por la conducta ejemplar ejercitada por los gerentes de mayor cargo y otros líderes. – Incentivos para fomentar y elementos disuasivos para hacer cumplir los comportamientos deseados. Existe un vínculo claro entre el comportamiento individual y el esquema de recompensas de recursos humanos que la empresa haya implementado. – Reglas y normas, las cuales proveen mayor guía sobre el comportamiento organizativo deseado. Esto se vincula en forma muy clara con los principios y políticas que la empresa haya implementado (Pág. 80)	- El éxito en la dirección de proyectos de una organización depende en gran medida de un estilo de comunicación efectivo dentro de la organización, sobre todo si se considera la globalización de la profesión de dirección de proyectos. Las capacidades de comunicación dentro de la organización tienen gran influencia en la forma en que se llevan a cabo los proyectos. En consecuencia, los directores de proyecto en ubicaciones distantes pueden comunicarse de manera más efectiva con todos los interesados relevantes dentro de la estructura de la organización para facilitar la toma de decisiones. Los interesados y miembros del equipo del proyecto también pueden utilizar comunicaciones electrónicas (incluidos correo electrónico, mensajería de texto, mensajería instantánea, redes sociales, videoconferencia y conferencia por Internet y otros medios electrónicos) para comunicarse formal o informalmente con el director del proyecto. (Pág.. 48) • La Gestión de las Comunicaciones del Proyecto incluye los procesos requeridos para asegurar que la planificación, recopilación, creación, distribución, almacenamiento, recuperación, gestión, control, monitoreo y disposición final de la información del proyecto sean oportunos y adecuados. Los directores de proyecto emplean la mayor parte de su tiempo comunicándose con los miembros del equipo y otros interesados en el proyecto, tanto si son internos (en todos los niveles de la organización) como externos a la misma. Una comunicación eficaz crea un puente entre diferentes interesados que pueden tener diferentes antecedentes culturales y organizacionales, diferentes niveles de experiencia, y diferentes perspectivas e intereses, lo cual impacta o influye en la ejecución o resultado del proyecto. (Pág.. 314) • Planificar la Gestión de las Comunicaciones: El proceso de desarrollar un enfoque y un plan adecuados para las comunicaciones del proyecto sobre la base de las necesidades y requisitos de información de los interesados y de los activos de la organización disponibles. • Gestionar las Comunicaciones: El proceso de crear, recopilar, distribuir, almacenar, recuperar	Las comunicaciones se realizan con base en los roles y responsabilidades establecidas en la matriz RACI.	No presenta relación con la temática.
13	**Políticas y directrices**	Pautas y/o prácticas para establecer políticas, normas y directrices para las temáticas relacionadas con el gobierno y gestión de las tecnologías y la información.	- El Gobierno Corporativo adecuado de la Tecnología de la Información puede ayudar a los directores a garantizar la conformidad con las obligaciones (reglamentarias, legislativas, de ley, contractuales) relacionadas con el uso aceptable de la Tecnología de la Información. (Pág. 8) - Las políticas deberían establecer una buena conducta en la utilización de la Tecnología de la información. (Pág. 14) - Los directores también deberían asegurarse de que la Tecnología de la Información cumple con las obligaciones externas (reglamentarias, legislativas, de ley, contractuales) y las prácticas laborales internas. (Pág. 14) PRINCIPIO 4: DESEMPEÑO (Pág. 17) Monitorear: los directores deberían monitorear la extensión hasta la cual se cumplen adecuadamente las políticas, como aquellas para la precisión de los datos y el uso eficiente de la Tecnología de la información PRINCIPIO 5: CONFORMIDAD (pág. 18) Evaluar Es recomendable que los directores evalúen con regularidad la extensión hasta la cual la Tecnología de la información satisface las obligaciones (reglamentarias, legislativas, de ley, contractuales), las políticas internas, las normas y las directrices profesionales. Los directores deberían también evaluar a intervalos regulares la conformidad interna de la organización con su sistema para el gobierno de la Tecnología de la información. Dirigir Los directores deberían dirigir a aquellos responsables de establecer mecanismos regulares y rutinarios para garantizar que el uso de la Tecnología de la información cumple con las obligaciones legislativas, de ley, contractuales), las normas y las directrices	- Catalizador : Principios, políticas y marcos de referencia son el vehículo para traducir el comportamiento deseado en guías prácticas para la gestión del día a día. (Pág. 27)	No presenta relación con la temática.	La gestión de servicios establece un conjunto de principios que complementan las funciones y procesos: - Especialización y coordinación: Los clientes deben especializarse en la gestión de su negocio y los proveedores en la gestión del servicio. El proveedor debe garantizar la coordinación entre los recursos y capacidades de ambos para tener el mejor balance. - Agencia: Los agentes actúan como intermediarios entre el cliente o usuario y el proveedor de servicios y son los responsables de la correcta prestación de dichos servicios. Estos deben de actuar siguiendo las indicaciones del cliente y protegiendo los intereses del cliente. los usuarios y los suyos propios. - Encapsulación: Los clientes y usuarios solo están interesados en la utilidad y garantía del servicio y no en los detalles técnicos o específicos para su correcta prestación. - Sistemas: Los sistemas son grupos de componentes interrelacionados o interdependientes que forman una unidad y colaboran entre sí para conseguir un objetivo común. (Strategy Pág. 34)	- Planificar (Establecer el SGCI) : Establecer la política los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización. - Hacer (Implementar y operar el SGSI): Implementar y operar la política, los controles, procesos y procedimientos del SGSI. - Verificar (Hacer seguimiento y revisar el SGSI): Evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y de reportar los resultados a la dirección, para su revisión. - Actuar (Mantener y mejorar el SGSI): Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI. (Pág. 9)
14	**Responsabilidad sobre la información**	Pautas y/o prácticas relacionadas con al definición de la propiedad, responsabilidad y uso de la información en la empresa.	- La norma establece un vocabulario para el gobierno de la Tecnología de la Información. (Pág. 8) - Uso de tecnología de la información. Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de la Tecnología de la Información para satisfacer las necesidades del negocio. Se incluyen tanto la demanda como el suministro de servicios de TI por parte de las unidades internas de negocios, unidades especialistas en TI o proveedores externos y empresas de servicios públicos (como los que suministran software). (Pág. 12) - Los directores deberían fomentar una cultura de buen gobierno de la Tecnología de la Información en su organización, exigiendo a la gerencia suministrar información oportuna para cumplir con la dirección y con los seis principios del buen gobierno. (Pág. 14) - Los directores deberían fomentar una cultura de buen gobierno de la Tecnología de la Información en su organización, exigiendo a la gerencia suministrar información oportuna para cumplir con la dirección y con los seis principios del buen gobierno. (Pág. 14)	- La información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios. (Pág. 13) - Catalizador: El catalizador información considera toda la información relevante para la empresa, no sólo la información automatizada. La información puede ser estructurada o desestructurada, formalizada o informal. (Pág. 81). - La información impregna toda la organización e incluye toda la información producida y utilizada por la empresa. La información es necesaria para mantener la organización funcionando y bien gobernada, pero a nivel operativo, la información es muy a menudo el producto clave de la empresa en sí misma.	No presenta relación con la temática.	La seguridad de la información es una actividad de gestión dentro de la marco de gobierno corporativo, que proporciona la dirección estratégica para las actividades de seguridad y garantiza se logran los objetivos. Se asegura, además, que la que los riesgos de seguridad de información se gestionan de manera adecuada y los recursos de información de la empresa se utilizan de forma responsable. El propósito de ISM (Information Security Management) es proporcionar un enfoque para todos los aspectos de TI seguridad y gestionar todas las actividades de seguridad de TI. (Introduction Pág. 82) La propiedad, responsabilidad y uso de la información de la empresa hace parte del gobierno corporativo y la gestión de servicios asegura que se proteja todo lo relacionado con la información.	La organización