APO 01

COBIT 5.0		ISO 27001		
APO 01	Gestionar el marco de gestión de TI	Requerimientos	Cobertura	Justificación
APO 01.01	Definir la estructura organizacional.	4.1 Entender la organización y su contexto	A+	El requerimiento 4.1 cubre este proceso en muchos aspectos. Ambos plantean la importancia de tener definida la estructura organizacional.
APO 01.02	Establecer roles y responsabilidades.	5.3 Roles organizacionales, responsabilidades y autoridades	C	El requerimiento 5.3 cubre este proceso completamente.
APO 01.03	Mantener los habilitadores del sistema de administración.		(N/A)	
APO 01.04	Comunicar objetivos y dirección de administración.	5.1 Liderazgo y Compromiso	A	Requerimiento 5.1 apartado d. se indica que se debe omunicar la importancia de la administración de la seguridad de la información.
		6.2 Objetivos de seguridad de información y planes para alcanzarlos.	A	Requerimiento 5.2 apartado d. se indica que los objetivos deben ser comunicados
		7.4 Comunicaciones	C	En este requerimiento se determinan los protocolos de comunicación y lo que debe ser comunicado
APO 01.05	Optimizar la colocación de la función de TI.		(N/A)	
APO 01.06	Definir información	7.5 Dcumentar Información /	A+	

	(datos) y propietarios del sistema .	7.5.1 General		
APO 01.07	Administrar la mejora continua de procesos.	10 Mejora / 10.2 Mejora continua	A+	
APO 01.08	Mantener la conformidad con políticas y procedimientos.	5. Politicas	A	En este requerimiento cubre lo referente a las politicas

APO02

COBIT 5.0		ISO 27001-2013 Draft		
APO02	Gestionar la Seguridad	Requerimientos	Cobertura	Justificación
APO02.01	Entender la dirección de la empresa	4.2) Comprendiendo las necesidades y expectativas de las partes interesadas	A+	La ISO indica que se tiene que comprender las necesidades de las partes interesadas y éstas deberán tener acceso a la información pertinente.

APO02.02	Evaluar el entorno actual, las capacidades y el rendimiento.	5.3) Roles organizacionales, responsabilidades y autoridades	A	La ISO nos indica que cada persona deberá tener la capacidad de asignar roles y responsabilidades de acuerdo a su capacidad
APO02.03	Definir las capacidades de TI y sus objetivos	6.1 Acciones para dirigir los riesgos y oportunidades, 6.1.2 Evaluacion de riesgos de seguridad de informacion	A-	la ISO nos indica que se deben evaluar los riesgos y las oporrtunidades para guiar el direccionamiento del negocio.
APO02.04	Conducir un análisis GAP.	No se puede mapear	(N/A)	No aplica
APO02.05	Definir el plan estratégico y el plan de proyectos y objetivos a seguir,	5) Liderazgo	A	La ISO nos indica que un manager de alto nivel debe asumir un liderazgo y un compromiso con los objetivos de la organización.
APO02.06	Comunicar la estrategia y la dirección de TI.	7.4) Comunicacion	A	La ISO nos indica que se debe de comunicar entre todas la partes interesadas.

APO03

COBIT 5.0		ISO 27001		
APO 03	Gestionar la Arquitectura Empresarial	Requisitos	Cobertura	Justificación
APO03.01	Desarrollar la visión de la Arquitectura Empresarial	-	-	La ISO no menciona el desarrollo de la visión de la Arquitectura Empresarial.
APO03.02	Definir la arquitectura de referencia	-	-	La ISO no menciona la definición de la arquitectura de referencia que describa la arquitectura actual y la planteada como objetivo.
APO03.03	Seleccionar oportunidades y soluciones	-	-	La ISO no menciona el proceso de selección.
APO03.04	Definir la implementación de la arquitectura	-	-	La implementación de la arquitectura empresarial no es mencionada en la ISO.
APO03.05	Proporcionar servicios de Arquitectura Empresarial	-	-	No se menciona el proceso de suministro de servicios, monitoreo o medición de la arquitectura empresarial.

COBIT 5.0		ISO 27001-2013 Draft		
APO04	Gestionar la Seguridad	Requerimientos	Cobertura	Justificación
APO04.1	Crear un ambiente propicio para la innovación.	No se puede mapear	(N/A)	No aplica
APO04.2	Mantener un entendimiento del ambiente de la empresa.	4.2) Comprendiendo las necesidades y expectativas de las partes interesadas	A+	La ISO indica que se tiene que comprender las necesidades de las partes interesadas y éstas deberán tener acceso a la información pertinente. Esto significa que deben de entender el ambiente de la Empresa.
APO04.3	Monitorear y observar el ambiente tecnológico.	9.1 Monitoreo, medicion, analisis y evaluacion	A-	Segun la ISO se deben monitorear los procesos de seguridad de la informacion y los controles que se realizan, se debe de saber quien monitorea los servicios y saber los resultados de dicho monitoreo.
APO04.4	Evaluar el potencial de tecnologías emergente y de ideas innovadoras.	No se puede mapear	(N/A)	No aplica
APO04.5	Recomendar más iniciativas apropiadas.	10.2) Mejora continua	A	La ISO indica que de manera perenne se debe de buscar mejoras a las tecnologías aplicadas. De esa forma se podrán hacer las recomendaciones de mejoras.

APO04.6	Monitorear la implementación y el uso de la innovación.	9.1 Monitoreo, medicion, analisis y evaluacion	A	Segun la ISO se deben monitorear los procesos de seguridad de la informacion y los controles que se realizan, se debe de saber quien monitorea los servicios y saber los resultados de dicho monitoreo.

APO05

COBIT 5.0		ISO 27001		
APO 05	Gestionar el portafolio	Requerimientos	Cobertura	Justificación
APO 05.01	Establecer la combinación de agentes de inversión	-	-	En la ISO no se habla nada sobre agentes de inversión
APO 05.02	Determinar la disponiblidad y fuentes de financiamiento	-	-	En la ISO no se habla nada sobre fuentes de financiamiento
APO 05.03	Evaluar y elegir programa a	7.1 Recursos /	A-	En ambos casos

	financiar	7.4 Comunicaciones		no se hablan de programas de financiamiento en sí, pero si del manejo de la información en todos los procesos de una organización. Sin embargo, en comunicaciones y recursos se habla sobre temas de manejo de los mismos.
APO 05.04	Monitorear, optimizar y reportar el desempeño del portafolio de inversión	9.1 Monitoreo, medición, análisis y evaluación	A-	Apartado b) Los métodos de monitoreo, medición, análisis y evaluación se deben aplicar para asegurar los resultados válidos.
APO 05.05	Mantenimiento de portafolios	-	-	ISO no menciona nada sobre algún "portafolio" y menos algún control estructurado de todos sus proyectos de TI, solo habla sobre el monitoreo a los sistemas de seguridad de la información.
APO 05.06	Gestión de beneficios logrados	9.3 Revisión de la gestión	A	Monitoreo y medición de resultados

				(aparatado c2); no conformidades y acciones correctivas (aparatado c1) ;y retroalimentación de las partes interesadas (aparatado d)

APO06

COBIT 5.0		ISO 27001		
APO 06	Gestionar el presupuesto y los costes	Requerimientos	Cobertura	Justificación
APO 06.01	Administrar finanzas y contabilidad	7.1 Resources	(A-)	No se hace referencia a finanzas, la parte de recursos es la más cercana
APO 06.02	Priorizar distribución de recursos	7.1 Resources	(A-)	No se hace referencia a finanzas, la parte de recursos es la más cercana
APO 06.03	Crear y mantener presupuestos	7.1 Resources	(A-)	No se hace referencia a finanzas, la parte de recursos es la más cercana
APO 06.04	Modelar y distribuir costos	7.1 Resources	(A-)	No se hace referencia a finanzas, la parte de recursos es la más cercana
APO 06.05	Administrar costos	7.1 Resources	(A-)	No se hace referencia a finanzas, la parte de recursos es la más cercana

APO07

COBIT 5.0		ISO 27001		
APO 07	Gestionar los Recursos humanos	Requerimientos	Cobertura	Justificación
APO 07.01	Matener una asignación de tareas adecuada y apropiada.	7.2 Competencias	A-	La sección competencias trata sobre aprovechar las habiilidades del personal. Para la asignación adecuada de tareas se debe tener en cuenta las competencias del personal.
APO 07.02	Identificar presonal de TI clave.	7.2 Competencias	A	La identificación de personal clave de TI también depende de las competencias que se busquen para los puestos principales relacionados a TI.
APO 07.03	Mantener las habilidades y competencias del personal.	7.2 Competencias	A+	El requerimiento 7.1 de la ISO equivale específicamente a este subproceso de COBIT.
APO 07.04	Evaluar el desempeño laboral del personal.	9.1 Monitoreo, medición, análisis y evalucación / 9.2 Auditoría Interna	A	Dentro del requerimiento correspondiente a la auditoría interna y el monitoreo se considera la evaluación del desempeño del personal.
APO 07.05	Planear y hacer seguimiento del uso de recursos humanos de TI y de negocio.	7.1 Recursos / 9.1 Monitoreo, medición, análisis y evalucación / 9.2 Auditoría Interna	A+	El planeamiento y administración de recursos humanos se considera parte del requerimiento 7.1 recursos. El seguimiento y evaluación se tratan en los requerimientos 9.1 y 9.2 enfocados al análisis y evaluación generales y a la auditoría interna de la emrpesa.
APO 07.06	Administrar personal de	7.2	A-	Se puede considerar el requerimiento de competencias de

	contrato.	Competencias		personal para este subproceso aun que la cobertura es pobre.

APO08

COBIT 5.0		ISO 27001-2013 Draft		
APO 08	Gestionar las Relaciones	Requerimientos	Cobertura	Justificación
APO08.01	Entender las expectativas del negocio	4.2 Comprendiendo las necesidades y expectativas de las partes interesadas	A	Pues se debe saber hacia donde va y apunta el negocio y la ISO indica que se tiene que comprender las necesidades de las partes interesadas
APO08.02	Identificar las oportunidades, riesgos y limitaciones de TI para mejorar el negocio	6.1 Acciones para dirigir los riesgos y oportunidades, 6.1.2 Evaluacion de riesgos de seguridad de informacion		la ISO indica que se deben planear y dirigir los riesgos y las orportunidades pra guiar el direccionamiento del negocio
APO08.03	Gestionar la relacion comercial		N/A	

APO08.04	Coordinar y comunicar	7.4 Comunicacion,	A	se deben de comunicar necesariamente los cambios realizados en las gestion de infotmacion para mantener integramente la seguridad.
APO08.05	Aportaciones a la mejora continua de los servicios	7.5.2 Creando y Actualizando, 10.2 Mejora continua	A+	Realizar simpre mejoras e la gestion de sistemas de seguridad de informacion y mantener siempre los documentos ordenados y bien documentados al alcance de todas las partes interesadas, ademas de comunicar las mejoras que se realicen

APO09

COBIT 5.0		ISO 27001		
APO 09	Gestionar los Contratos de Servicios	Requerimientos	Cobertura	Justificación
APO09.01	Identificar los servicios de IT	6.1 Acciones para dirigir los riesgos y oportunidades	A	El marco dice que se debe estudiar y analizar la demanda de los servicios de TI, y la iso dice que

				siempre se deben de identificar los riegos y planear los posibles efectos de estos riesgos
APO09.02	Catalogo de servicios permitidos por IT	7.5.3 Control de la informacion documentada	A	Segun la ISO se debe de tener documentada la informacion de la que se dispone, esta debe de estar adecuada y disponible, ademas de estar siempre protegida cintra perdida y legitimibilidad
APO09.03	Definir y preparar los acuerdos de servicio		N/A	
APO09.04	Monitorear y reportar los niveles de servicio	9.1 Monitoreo, medicion, analisis y evaluacion		Segun la ISO se deben monitorear los procesos de seguridad de la informacion y los controles que se realizan, se debe de saber quien monitorea los servicios y saber los resultados de dicho monitoreo
APO09.05	Revisar los acuerdos y contratos de servicios		N/A	

APO10

COBIT 5.0		ISO 27001		
APO 10	Gestionar los Proveedores	Requisitos	Cobertura	Justificación
APO10.01	Identificar y evaluar las relaciones y contratos con el proveedor	4.2 Comprendiendo las necesidades y expectativas de las partes interesadas	A	La ISO menciona la tarea de conocer las necesidades de las partes interesadas,

				incluyendo los contratos. Sin embargo, no llega al nivel de detalle que lo definido en COBIT.
APO10.02	Seleccionar proveedores	-	-	La ISO no menciona el proceso de selección de proveedor.
APO10.03	Gestionar las relaciones y contratos con el proveedor	A.15.2.2 Gestión de cambios de los servicios del proveedor	C	La ISO, al igual que COBIT, menciona la necesidad de gestionar permanentemente la información del proveedor. Manteniendo y mejorando la misma, cada vez que sea necesario.
APO10.04	Gestionar el riesgo del proveedor	-	-	La ISO no contempla la identificación y manejo del riesgo relacionado a la capacidad de los proveedores de brindar sus servicios continuamente.
APO10.05	Monitorear el desempeño y cumplimiento del proveedor	A.15.2.1 Monitoreo y revisión de los servicios del proveedor	C	La ISO, al igual que COBIT, menciona la necesidad de monitorear y auditar regularmente los servicios

				brindados por el proveedor

APO11

COBIT 5.0		ISO 27001-2013 Draft		
APO 11	Gestionar la Calidad	Requerimientos	Cobertura	Justificación
APO11.01	Establecer un sistema de gestión de la calidad.	No se puede mapear	N/A	La ISO no menciona el tema de Gestión de Calidad
APO11.02	Definir y gestionar los estándares, prácticas y procedimientos de calidad.	No se puede mapear	N/A	La ISO no menciona procedimientos de calidad.
APO11.03	Enfocar la gestión de calidad hacia los clientes	No se puede mapear	N/A	La ISO no menciona aspectos de enfoques de calidad hacia clientes
APO11.04	Ejecutar monitoreo, control y revisiones de la calidad.	No se puede mapear	N/A	La ISO no menciona algúna forma de seguimiento de calidad.
APO11.05	Integrar la gestión de la calidad en la entrega de soluciones para el desarrollo y el servicio.	No se puede mapear	N/A	La ISO no menciona la integración de la calidad.
APO11.06	Gestionar la mejora continua.	5.1 (liderazgo y Compromiso), 5.2 (Política),6(Planeamiento),7.1(Soporte-Recrusos) y 10.2 (Mejora Contínua)	A	La ISO menciona principalmente la mejora continua en el aspecto de la seguridad de información. En el punto 5.1.g) Principalemente nos habla del liderazgo y compromiso

				de los gerentes frente a la mejora continua de la empresa abocandose en la Seguridad de Información; esto se complementa con el punto 5.2.d) el cual nos menciona el compromiso frente a la mejora continua. En la parte 6 de Planeamiento nos menciona que se debe incetivar la mejora continua al igual que la parte 7 de Soporte nos habla de implementar y manter la mejora continua en la Empresa basadonse otra vez en la Seguridad de Información. En síntesis la sección 10 (Mejora) en la especificación 10.2 Nos habla de la mejora continua como tal centrandose nuevamente enla seguridad e Información más no menciona otros aspectos de mejora.

APO12

COBIT 5.0		ISO 27001		
APO 12	Gestionar el Riesgo	Requerimientos	Cobertura	Justificación
APO 12.01	Recolectar data	-	-	ISO no menciona ningún requerimiento referente a la identificación de riesgos en los procesos que maneja la organización
APO 12.02	Analizar el riesgo	8.2 Evaluación	A+	Considera la

		de riesgos de seguridad de información		evaluación de los riesgo en un determinado intervalo para determinar como se ven afectados ante algún cambio u ocurrencia.
APO 12.03	Mantener el portafolio del riesgo	-	-	ISO no menciona nada sobre mantener un portafolio o inventario de los riesgos más frecuentes o conocidos en la organización.
APO 12.04	Articular el riesgo	9.3 Revisión de la gestión	C	Considera el resultado de la evaluación de riesgos y el estado del riesgo luego del plan de tratamiento.
APO 12.05	Definir un portafolio de gestión de riesgos	6.1 Acciones para abordar los riesgos y oportunidades	A+	Planifica acciones para abordar los riesgos y oportunidades y como integrarlos en los procesos de gestión de la seguridad de información. Asimismo, evalua la efectividad de estas acciones.
APO 12.06	Respuesta al riesgo	8.3 Tratamiento de riesgos de seguridad de información	C	Considera la implementación del plan de tratamiento de riesgos de seguridad de información

APO13

COBIT 5.0		ISO 27001-2013 Draft		
APO 13	Gestionar la Seguridad	Requerimientos	Cobertura	Justificación
APO13.01	Establecer y mantener un SGSI (Sistema de Gestión de Seguridad de la Información).	4(Contexto de la Organización), 5(Liderazgo),6(Planeamiento), 7(Soporte) y 9(Evaluación de Performance)	E	La ISO 27001 nos habla pricipalmente del ámbito de la seguridad de la Información en la Empresa por lo que los grandes aspectos de esta corresponden a lo expuesto en COBIT. Empezamos por que se define las características,alcances y límites de lo que sería el Sistema de Gestión de Seguridad de Infromación(SGSI) y su la forma en que se debe implemntar en la Empresa.Se expresa a su vez que este sistema debe ir alineado a las políticas de la empresa, contexto organizacional y objetivos; esto va también con la alineación de este sistema con la gestión de seguridad general en la Empresa y a su vez con los requerimientos de esta. También nos menciona de la importancia de la comunicación del sistema y su difusión por toda esta tanto la forma como los responsables.
APO13.02	Definir y administrar un plan de tratamiento de riesgos de la seguridad de la información.	6(Planeamiento):Principalmente 6.1 y 6.2 en un pequeño aspecto. **8.2, 8.3(Principales)** y 9.3	A+	Se menciona con alto detalle como el plan de seguridad de información va a manejar los riesgos en la empresa, con un plan estructurado que va alineado a los casos de negocio de la empresa. Es importante reslatar que nos mencionan lo importnate de que el control de riesgos sea óptimo para esto debe estar asociada a los objetivos y recursos empresariales. La norma describe de que manera se proporcionara información para el correcto desarrollo de este plan. Importante es mencionar que no se especifica la forma en que se va a

				medir la efectividad de las prácticas escogidas aunque si mencionan su importancia, y se menciona vagamente la recomendación de programas de capacitación de la seguridad de información.
APO13.03	Monitorear y revisar el SGSI.	7(Soporte),**9(Performance evaluation)**,10 (Mejora)	E	Se menciona explicitamente lo referido al monitoreo y la revisión del Sistema de Gestión de Seguridad de Información. Principlamente en la revisión periódica del SGSI para poder corregir aspectos importantes, para esto se menciona la importancia de recolectar y analizar información continuamente. Se menciona el tema de auditorías internas, así como la realziación de examenes para medir el grado de efectividad de SGSI actual. Además, estipula que se debe proporcionar información pertienete para el mantenimiento ya que esto nos ayudara a tener resultados correctos del seguimiento; nos habla también de guardar acciones que podrían tener impacto en el redimiento del SGSI en la empresa.