ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Proyecto de Grado para la obtención del título de Magister en Evaluación y Auditoría de Sistemas Tecnológicos

EVALUACIÓN TÉCNICA DEL GOBIERNO CORPORATIVO DE TI EN LA DIRECCIÓN PROVINCIAL DEL CONSEJO DE LA JUDICATURA DE PICHINCHA

Christian Carrasco Quelal
Fausto Naranjo Calderón

Temario

1. Objetivos
   - General.
   - Específicos.
2. Justificación.
3. Planteamiento del problema.
4. Evaluación técnica.

Temario

1. Objetivos
   - General.
   - Específicos.
2. Justificación.
3. Planteamiento del problema.
4. Evaluación técnica.

Objetivo - General

Realizar la evaluación técnica del Gobierno de TI en la Dirección Provincial del Consejo de la Judicatura de Pichincha mediante las directrices y procedimientos de COBIT versión 5, para recomendar mejoras en los servicios de TI ofrecidos a los diferentes actores internos y externos de la institución.

Objetivos - Específicos

- Evaluar el establecimiento y mantenimiento del marco de gobierno de TI para recomendar un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa.

- Evaluar cómo optimiza el área de TI el valor de sus procesos, servicios y activos para que las necesidades del negocio sean soportadas efectiva y eficientemente basada en recomendaciones de buenas prácticas de TI.

- Evaluar si los recursos de TI se encuentran disponibles cuando los procesos del negocio lo requieran.

- Evaluar la medición y elaboración de informes en cuanto a conformidad y desempeño de TI de la institución si son claros y transparentes.

- Entregar un informe de evaluación técnica para mejorar los procesos relacionados a gobierno de TI en la institución.

Temario

1. Objetivos
   - General.
   - Específicos.
2. Justificación.
3. Planteamiento del problema.
4. Evaluación técnica.

Justificación

El Departamento de informática de la Dirección Provincial del Consejo de la Judicatura de Pichincha requiere se realice una evaluación técnica a los procesos de gobierno de tecnología con el fin de mejorar sus procesos y servicios tecnológicos para afrontar los nuevos desafíos institucionales, y plantear un lineamiento para llegar a certificar sus procesos de TI.

Temario

1. Objetivos
   - General.
   - Específicos.
2. Justificación.
3. Planteamiento del problema.
4. Evaluación técnica.

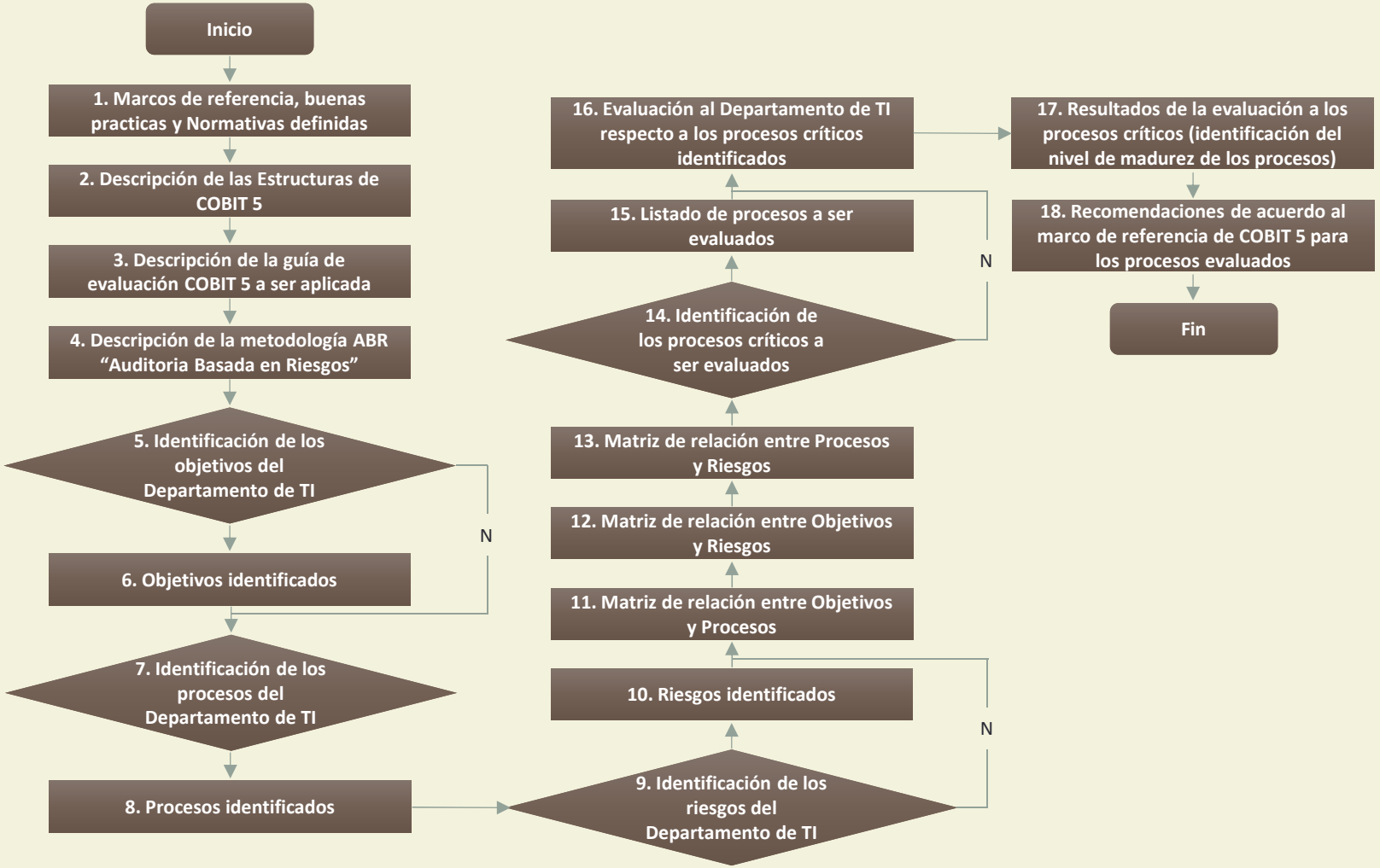
Planteamiento del problema

- No contar con infraestructura civil propia.
- La falta de recurso humano calificado.
- Falta de comunicación entre las diferentes áreas de la institución y con el área de TI.
- Limitación en la entrega de recursos de TI.
- Falta de una estructura organizacional de TI a nivel nacional y provincial.
- Existe desconocimiento de la alta gerencia sobre la importancia estratégica de TI.
- Problemas con la funcionalidad de los sistemas de información.

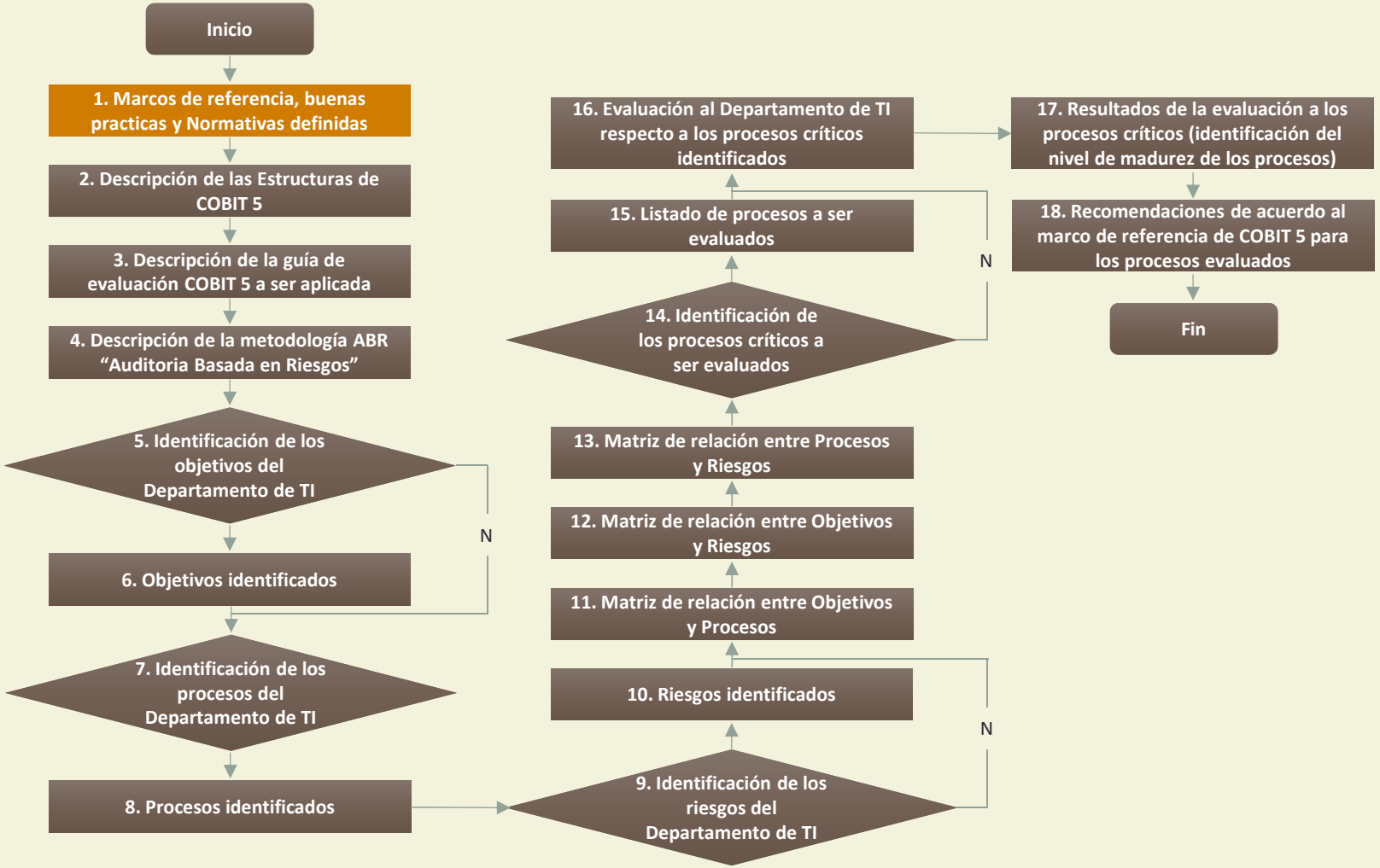
Temario

1. Objetivos
   - General.
   - Específicos.
2. Justificación.
3. Planteamiento del problema.
4. Evaluación técnica.

Evaluación Técnica



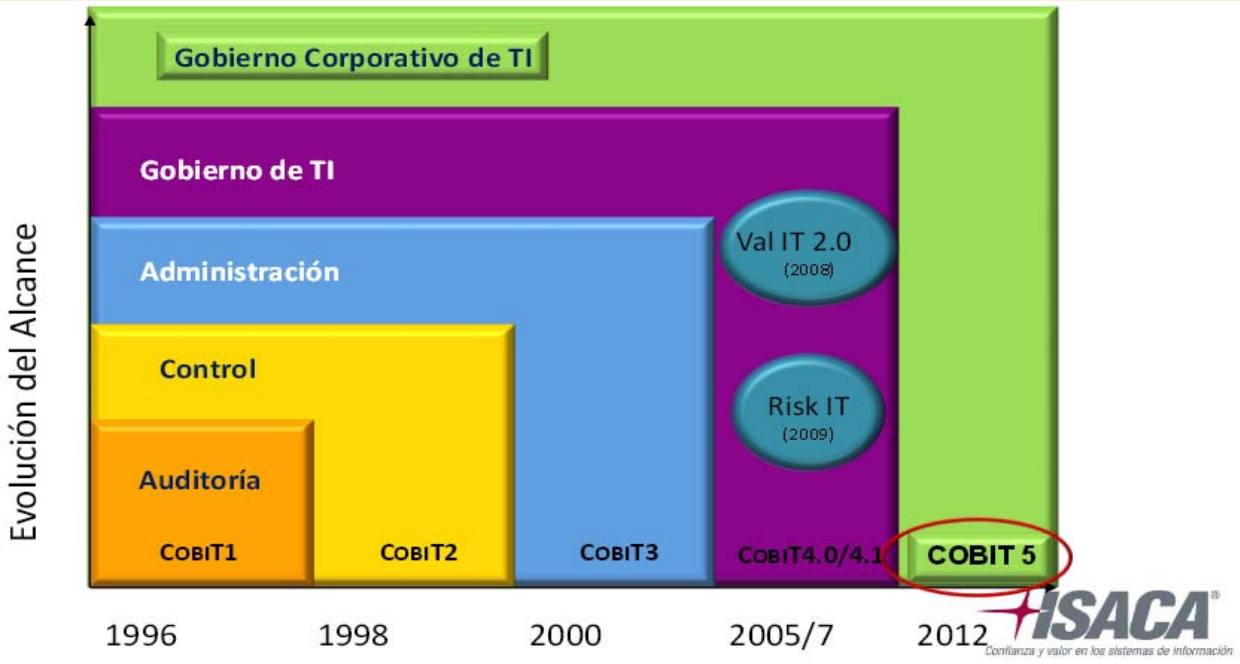
Evaluación Técnica



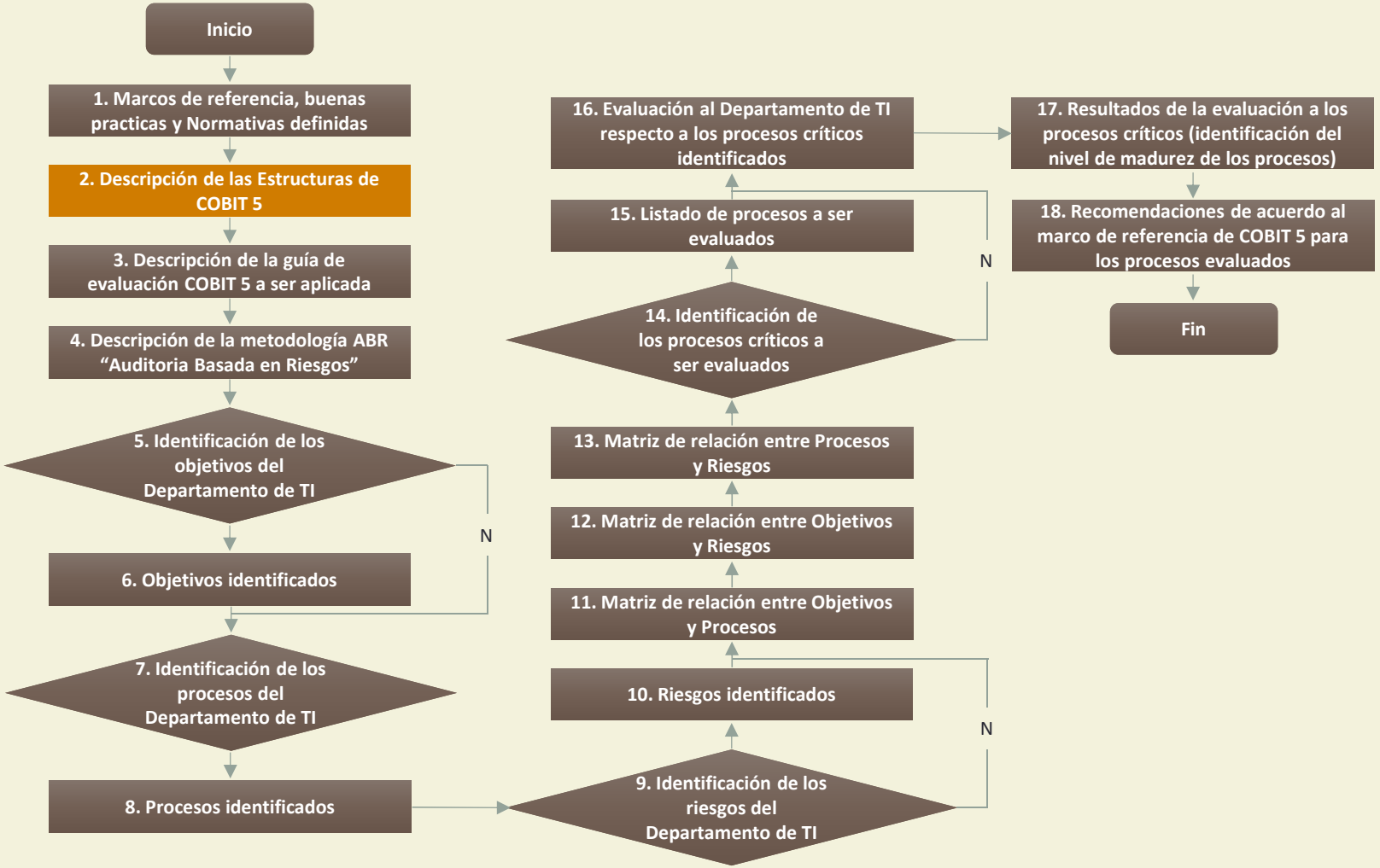
1. Marcos de referencia, buenas practicas y Normativas definidas

COBIT v5

- Objetivos de Control para Información y Tecnologías Relacionadas.
- Es desarrollado y mantenido ISACA y IT Governance Institute.
- ISO/IEC 38500.



Evaluación Técnica



2. Descripción de las Estructuras de COBIT 5

Gobierno TI

EDM Evaluar, Orientar, Supervisar

- EDM01 Marco Gobierno TI
- EDM02 Entrega de Beneficios
- EDM03 Optimizar Riesgo
- EDM04 Optimizar Recursos
- EDM05 Transparencia hacia partes interesadas

Gestión de TI

APO Alinear, Planificar, Organizar

- APO01 Marco Gestión TI
- APO02 Gestionar Estrategia
- APO03 Arquitectura Empresarial
- APO04 Gestionar Innovación
- APO05 Gestionar Cartera
- APO06 Presupuesto Costes
- APO07 Recursos Humanos
- APO08 Gestionar Relaciones
- APO09 Acuerdos de Servicio
- APO10 Gestionar Proveedores
- APO11 Gestionar Calidad
- APO12 Gestionar Riesgo
- APO13 Gestionar Seguridad

BAI Construir, Adquirir, Implementar

- BAI01 Programas y Proyectos
- BAI02 Definición de Requisitos
- BAI03 Construcción de requisitos
- BAI04 Disponibilidad y capacidad
- BAI05 Cambio Organizativo
- BAI06 Gestionar Cambios
- BAI07 Aceptación cambio
- BAI08 Gestionar Conocimiento
- BAI09 Gestionar Activos
- BAI10 Gestionar Configuración

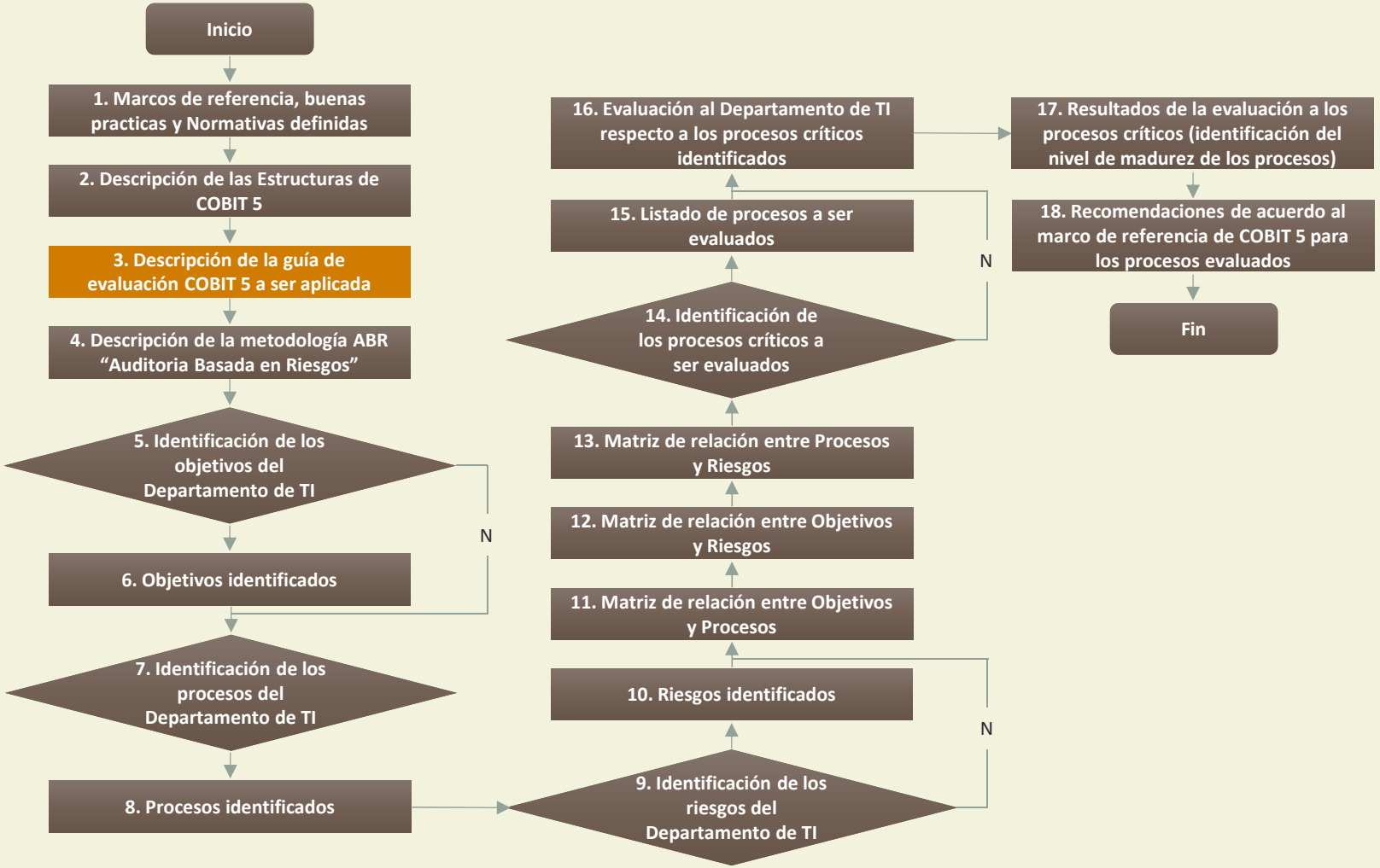
DSS Entregar, Dar Servicio, Soporte

- DSS01 Gestionar las operaciones
- DSS02 Incidentes de Servicio
- DSS03 Gestionar Problemas
- DSS04 Continuidad Servicio
- DSS05 Servicios de Seguridad
- DSS06 Controles de Procesos

MEA Supervisar, Evaluar, Valorar

- MEA01 Rendimiento y Conformidad
- MEA02 Control Interno
- MEA03 Requerimientos Externos

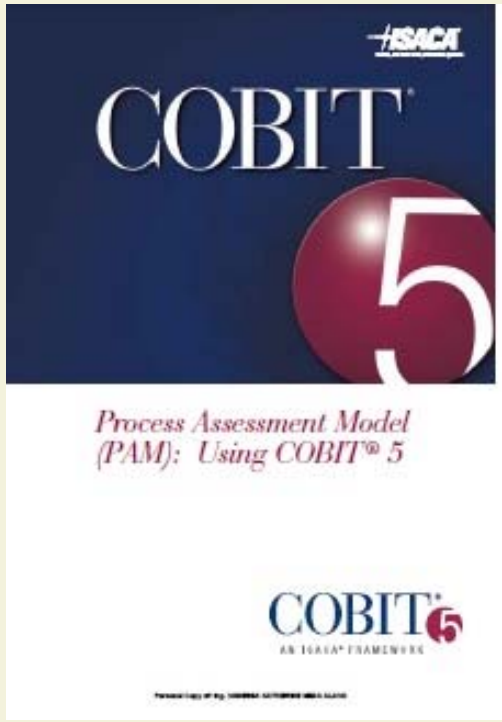
Evaluación Técnica



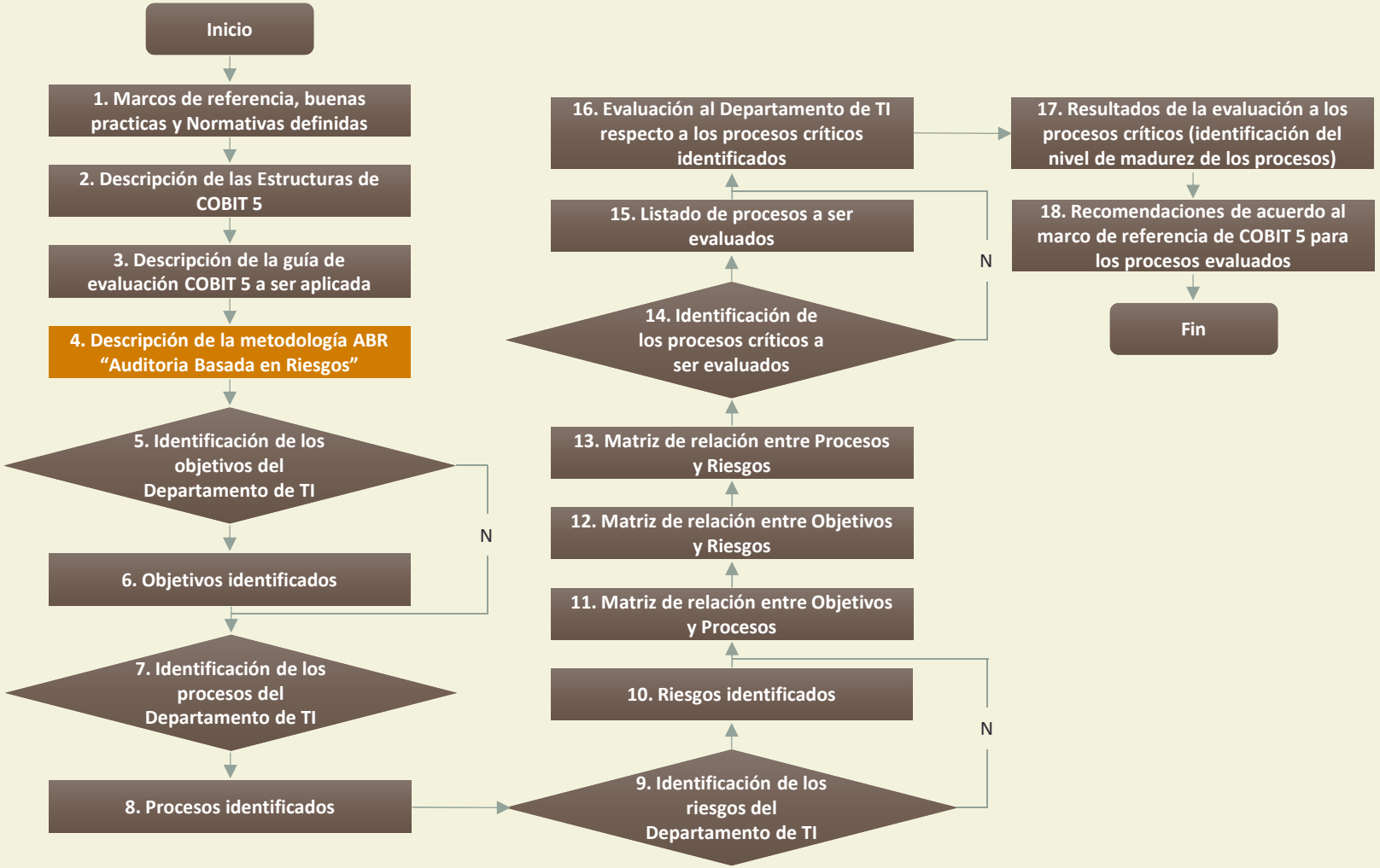
3. Descripción de la guía de evaluación COBIT 5 a ser aplicada

Modelo de Procesos de Evaluación PAM:

- Control más exhaustivo y exigente.
- Basado en evidencias.



Evaluación Técnica



4. Descripción de la metodología ABR "Auditoria Basada en Riesgos"

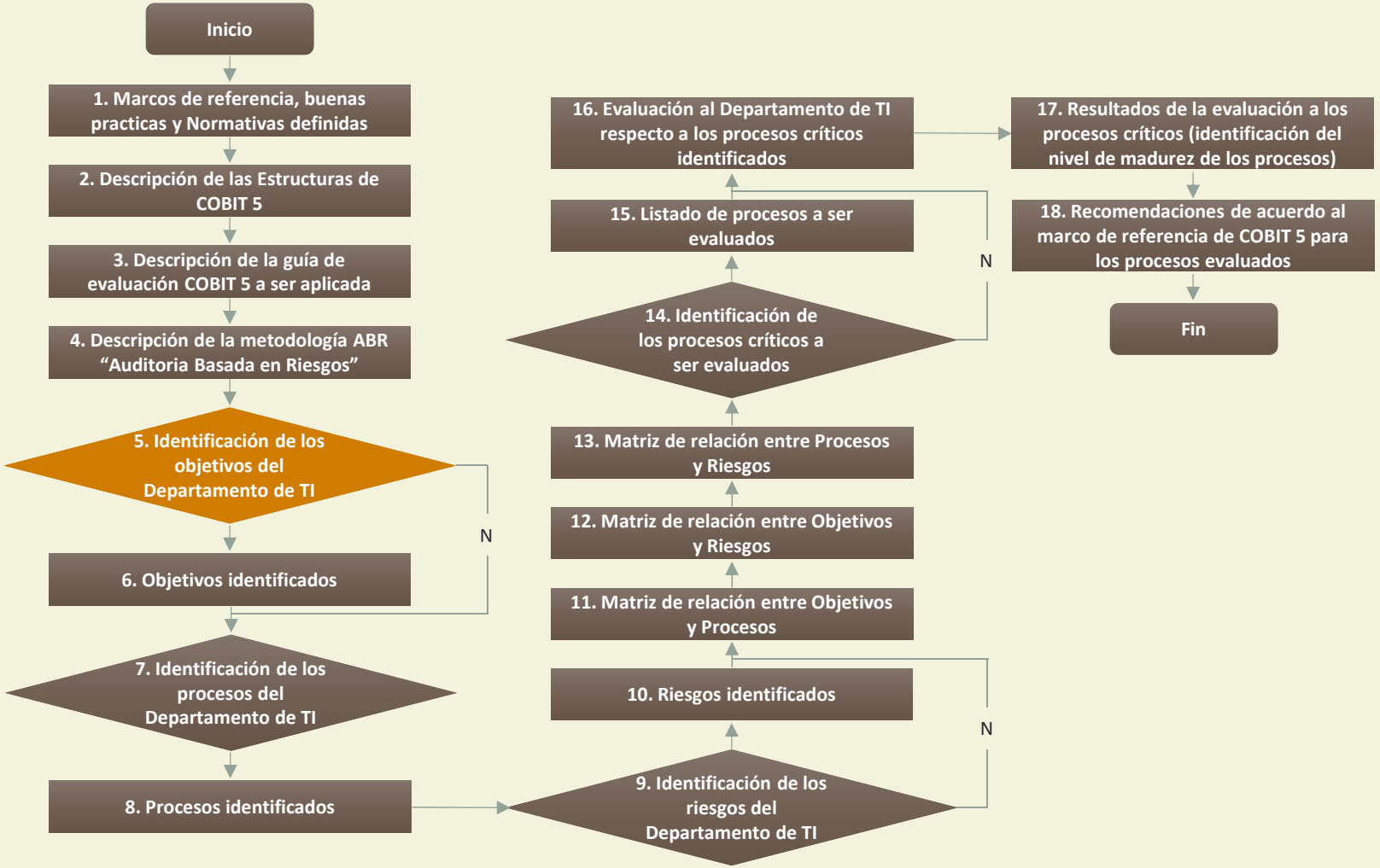
- **Fases de la metodología de investigación ABR**:

  a. Comprensión de Objetivos y Procesos de negocio relacionados
  b. Identificación de Objetivos y Riesgos
  c. Evaluación de Riesgos
  d. Análisis de Procesos y Riesgos
  e. Definición del plan

- **Técnicas de investigación de campo.**

- **Lugar.**

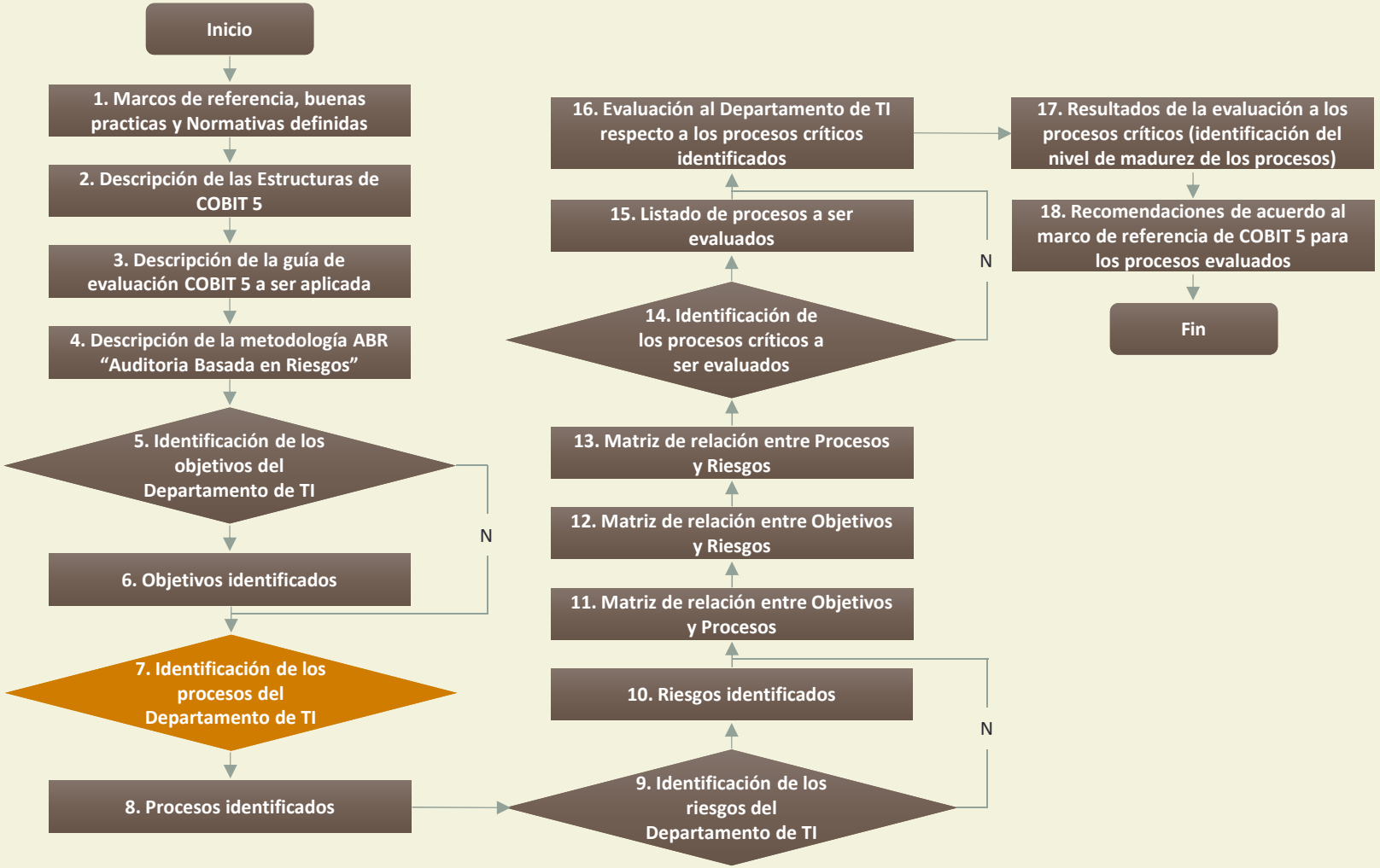
Evaluación Técnica



5. Identificación de los objetivos del Departamento de TI

ID	DESCRIPCIÓN
O1	Implementar redes de área local (LAN's), en las dependencias de propiedad de la Función Judicial.
O2	Implementar redes de área local inalámbricas (WLAN's), en las dependencias arrendadas por la Función Judicial.
O3	Implementar redes de área metropolitana (MAN's) en los diferentes cantones de la Dirección Provincial.
O4	Implementar una red provincial de telecomunicaciones, red de área metropolitana (MAN), que proporcione y comparta información de video conferencia, telefonía IP y datos etc.
O5	Adquirir servidores, equipos de telefonía IP y video conferencia e infraestructura robusta, para todas las dependencias Judiciales y Administrativas de la Dirección Provincial.
O6	Adquirir sistemas de seguridad electrónicos y de software, para preservar la información en las diferentes dependencias Judiciales y Administrativas.
O7	Adquirir sistemas de seguridad electrónicos y de software, para preservar la información en las diferentes dependencias Judiciales y Administrativas.
O8	Adquirir equipamiento informático de última tecnología, para usuarios finales de la Institución.
O9	Implementar el Sistema Automático de Trámite Judicial Ecuatoriano (SATJE) estándar, en todas las dependencias Judiciales de la Dirección Provincial.
O10	Implementar el módulo quejas del SATJE, en todas las Unidades de Control Disciplinario de la Dirección Provincial.
O11	Implementar el portal Web de la Dirección Provincial, que permita publicar toda la información que exige la ley de trasparencia y libre acceso a la información.
O12	Implementar un sistema de flujo documental, para hacer el seguimiento de los procesos en todas las áreas administrativas de la Dirección Provincial.
O13	Implementar sistemas estadísticos, para la toma de decisiones de las autoridades de la Dirección Provincial y dotar de información en tiempo real al público que solicite.
O14	Implementar sistemas financieros, de recursos humanos y administrativos, para las diferentes dependencias de la Dirección Provincial.
O15	Brindar herramientas informáticas de consulta jurídica a los Funcionarios Judiciales de la Dirección Provincial.
O16	Brindar un soporte técnico rápido y adecuado al Funcionario Judicial.
O17	Mantener el parque informático en perfectas condiciones, para que los Funcionarios Judiciales se desenvuelvan bien en sus actividades.
O18	Mantener capacitado a los Funcionarios Judiciales, en el manejo de los sistemas informáticos.
O19	Colaborar en la transformación de la Función Judicial en un modelo y ejemplo de organización, calidad de servicio, eficiencia, modernidad, economía y seguridad.

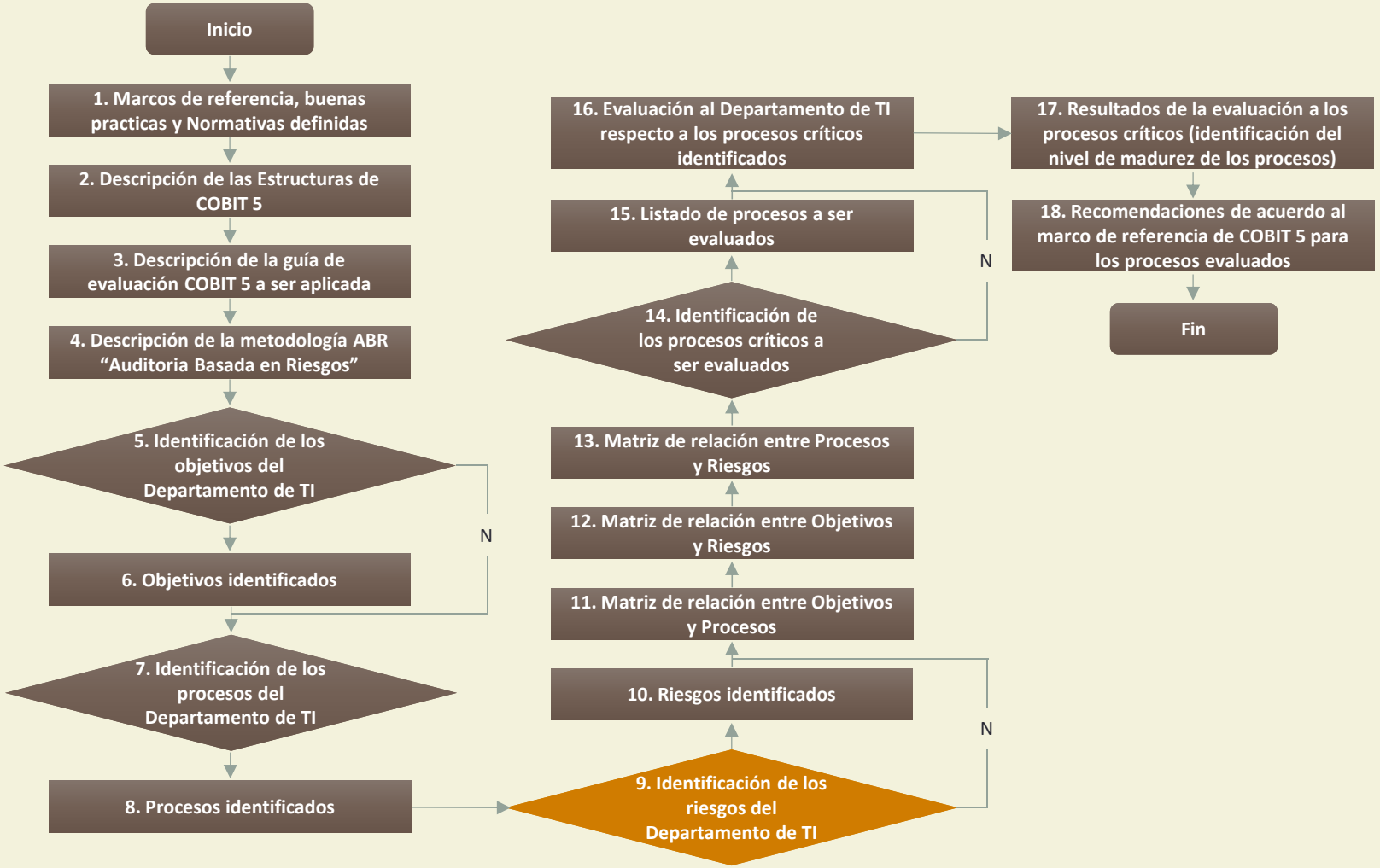
Evaluación Técnica



7. Identificación de los procesos del Departamento de TI

ID	DESCRIPCIÓN
P1	Desarrollo de proyectos en telecomunicaciones.
P2	Administración de redes y telecomunicaciones.
P3	Seguridad de información e infraestructura.
P4	Desarrollo de sistemas informáticos.
P5	Administración y mantenimiento de sistemas informáticos.
P6	Adquisición de equipos y de servicios informáticos (HW / SW).
P7	Soporte técnico.
P8	Digitación.

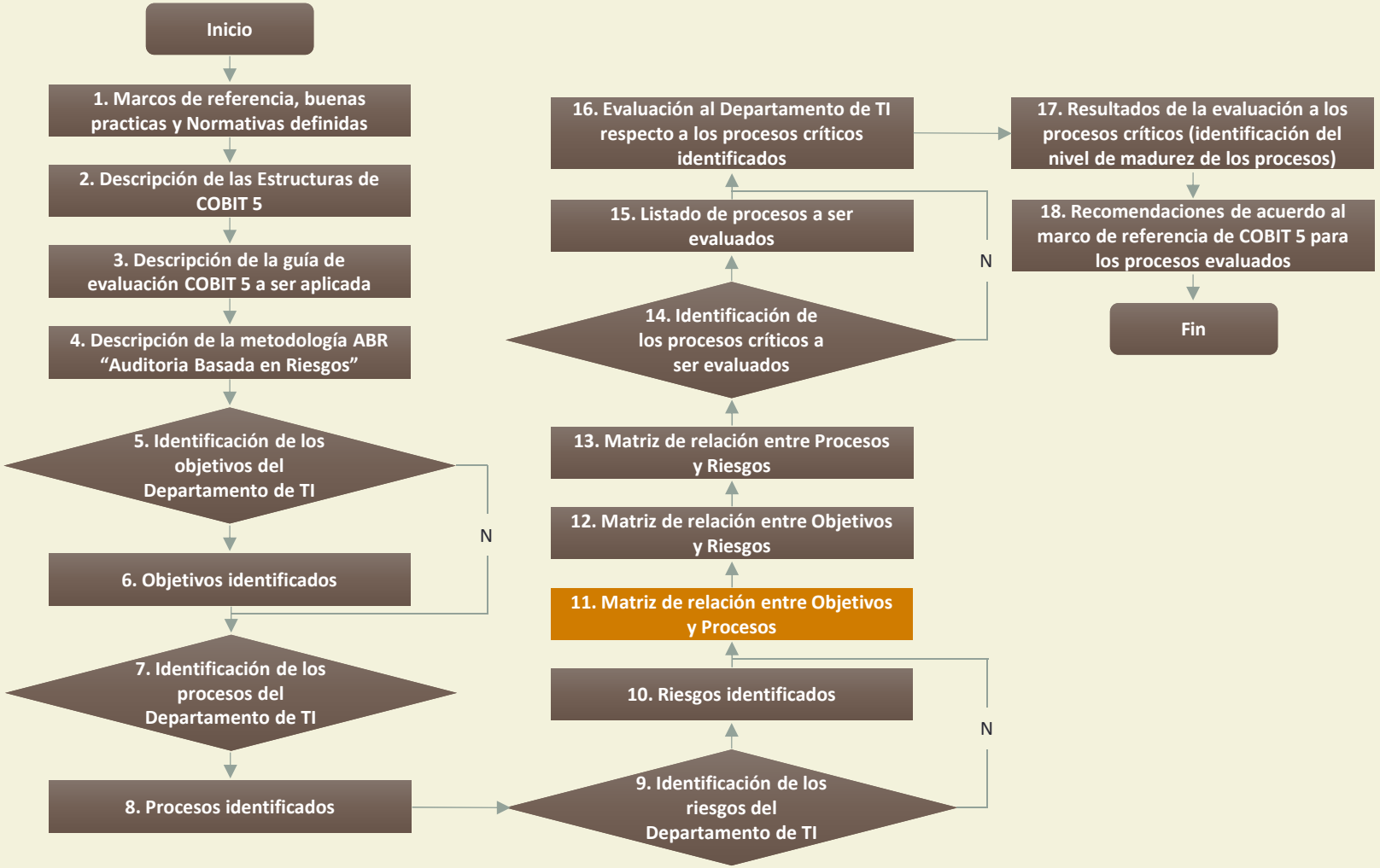
Evaluación Técnica



9. Identificación de los riesgos del Departamento de TI

ID	DESCRIPCIÓN
R1	Paralización de los servidores de Bases de Datos.
R2	Paralización de los servidores de Aplicaciones.
R3	Paralización de los enlaces de telecomunicaciones.
R4	Atención tardía en el soporte técnico a los Funcionarios Judiciales.
R5	Utilización inadecuada de los sistemas informáticos por parte de los Funcionarios.
R6	No disponibilidad de la aplicación SATJE.
R7	No disponibilidad del servicio de Internet.
R8	No disponibilidad del servicio de Correo.
R9	No disponibilidad del servicio de Telefonía.
R10	Fallo del Switch Principal.
R11	Fallo del servidor de Directorio Activo.
R12	No disponibilidad del servidor de Archivos.
R13	No tener actualizado el servidor de Antivirus.
R14	No disponibilidad del servidor web.
R15	Fallo del equipo de seguridad perimetral (Firewall).
R16	Fallo en el sistema de enfriamiento para el Data Center.
R17	Fallo en la seguridad física.
R18	No disponer de presupuesto para la ejecución de proyectos.

Evaluación Técnica

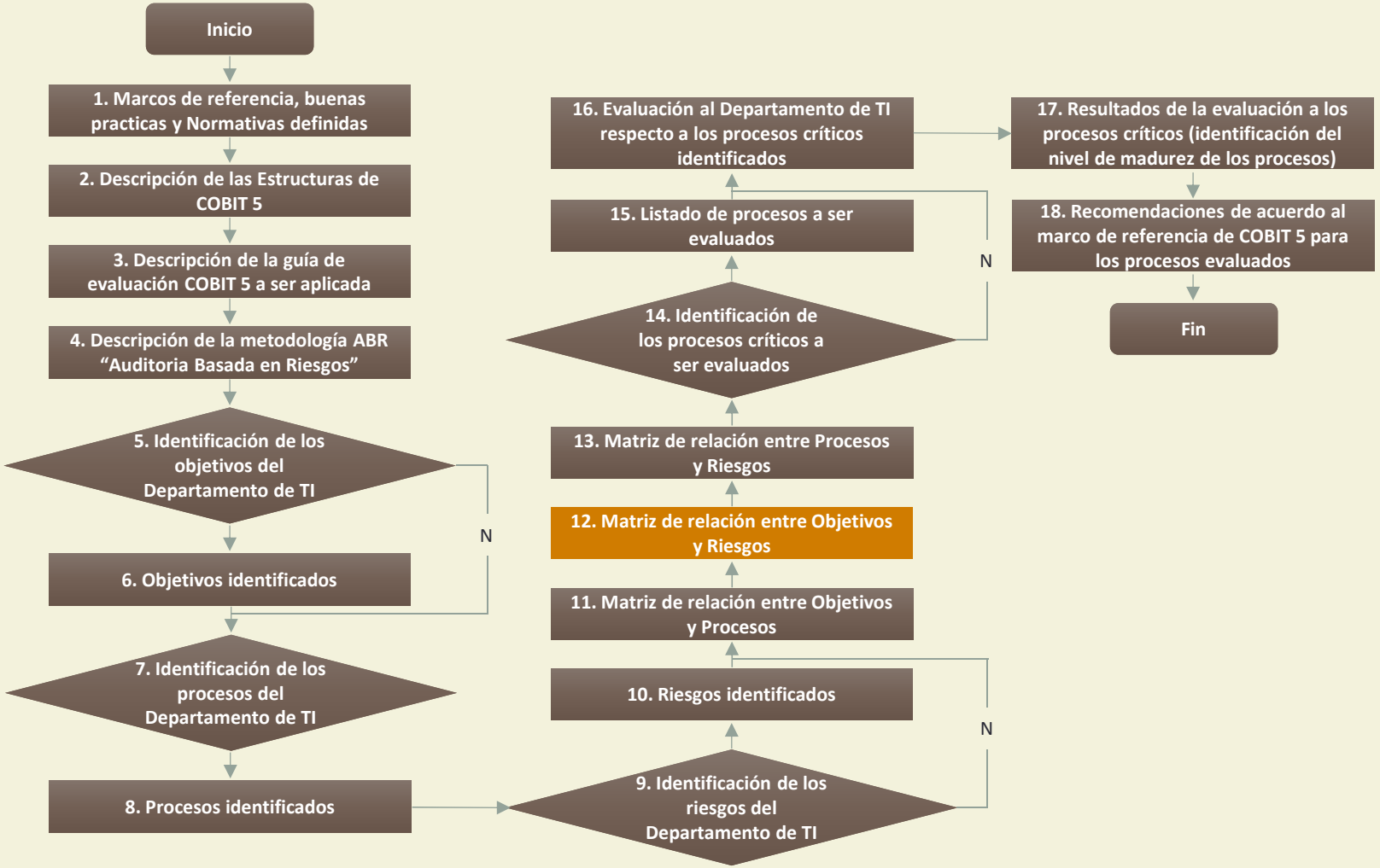


11. Matriz de relación entre Objetivos y Procesos

Evidenciar los procesos requeridos para cumplir cada uno de los objetivo de TI:

		PROCESOS							
		P1	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**
OBJETIVOS	**O1**	X	X	X		X			
	O2	X	X	X		X			
	O3	X	X	X		X			
	O4	X	X	X		X			
	O5						X		
	O6			X			X		
	O7						X		
	O8					X			
	O9					X			
	O10			X	X				
	O11			X	X				
	O12			X	X				
	O13			X	X				
	O14			X			X		
	O15							X	
	O16					X		X	
	O17							X	
	O18	X	X	X	X	X	X	X	X

Evaluación Técnica

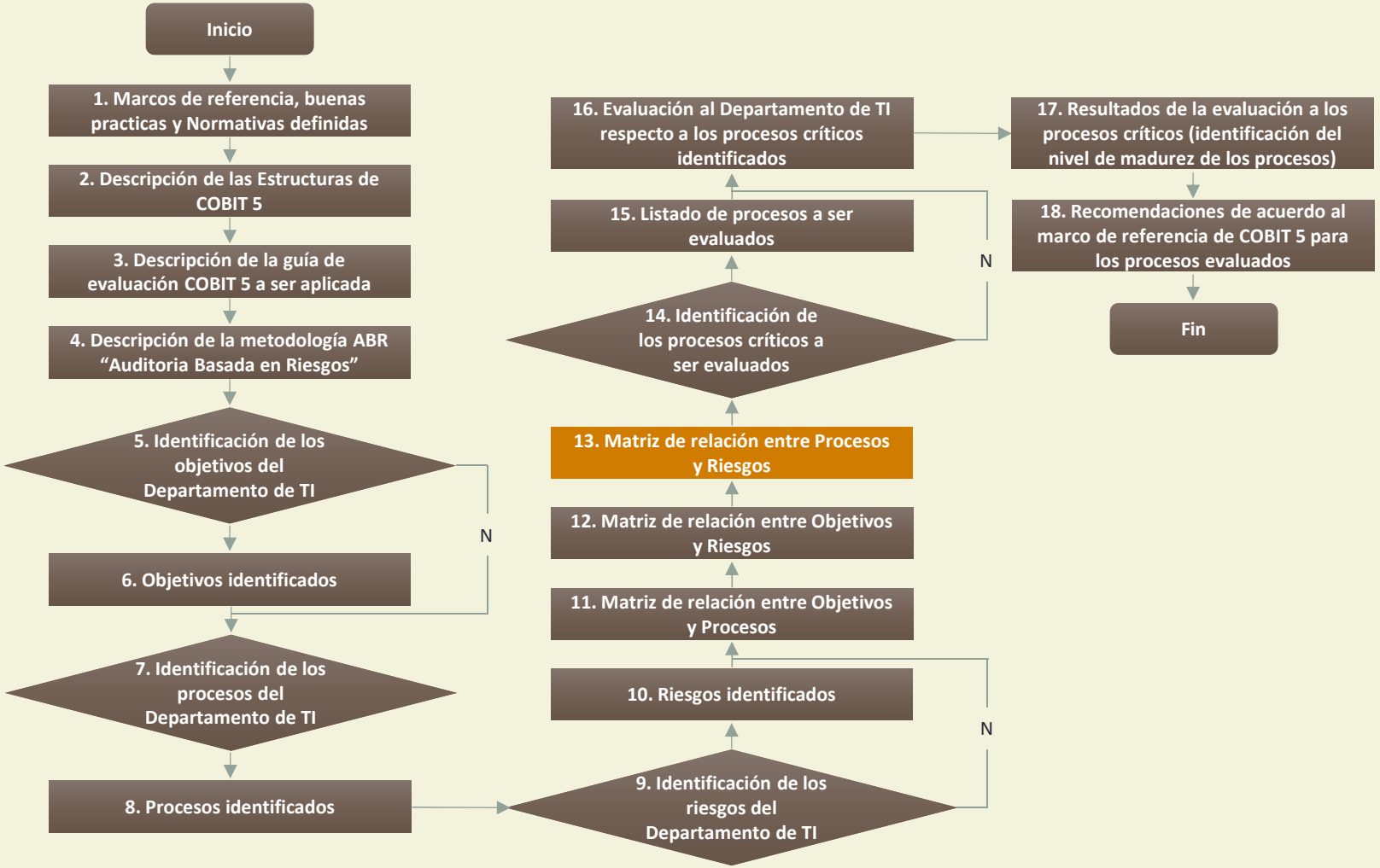


12. Matriz de relación entre Objetivos y Riesgos

Identificar cuáles son los objetivos con mayor consideración para su cumplimiento:

		RIESGOS																
		R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18
OBJETIVOS	O1										X						X	X	
	O2										X						X	X	
	O3			X							X					X	X	X	
	O4			X							X					X	X	X	
	O5																X	X	X
	O6																X	X	X
	O7																		X
	O8	X	X		X		X					X	X	X					
	O9	X	X		X		X					X	X	X					
	O10	X	X		X		X	X					X	X	X	X			
	O11	X	X		X							X							
	O12				X	X													
	O13				X	X													
	O14				X														X
	O15				X				X	X		X	X						
	O16				X											X	X	X	
	O17				X				X			X	X	X					
	O18	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Evaluación Técnica



13. Matriz de relación entre Procesos y Riesgos

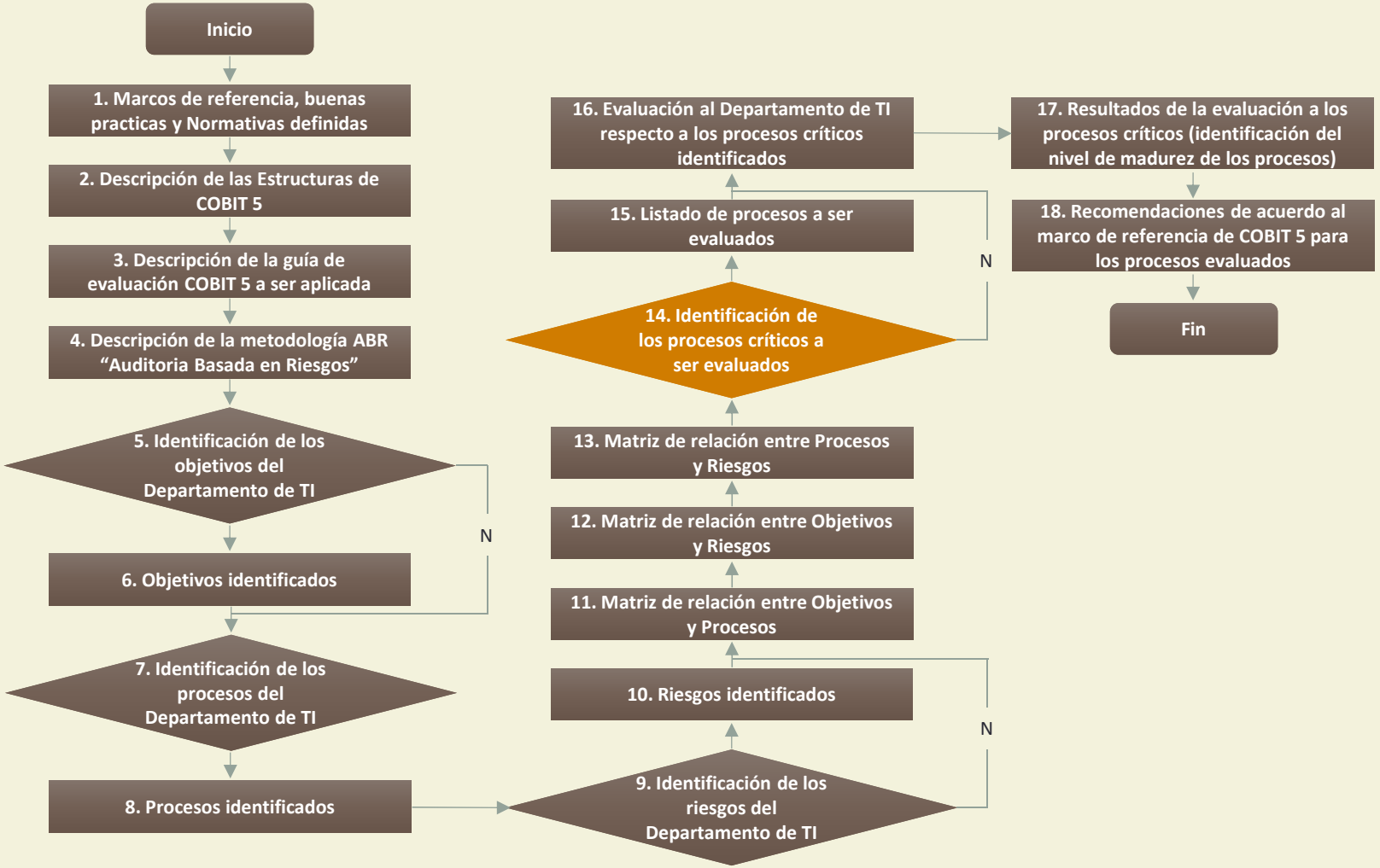
Identificar los procesos más críticos de TI de acuerdo a los riesgos con los que están relacionados cada uno de ellos:

		RIESGOS																	Totales	
		R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R18	C	S
PROCESO	P1			C							C								S	2	1
	P2			C	S	S				C	C								S	3	3
	P3	C	C	C		S	C	S	S	S	C	C	S	C	S	C	C	C		10	6
	P4	C	C	C	S		S	S	S		C	C			C		C		S	7	5
	P5	C	C	C	C		S	S	S		C	C	S		C		C		S	8	5
	P6				C				S	S								S	C	2	3
	P7				C				S	S								S		1	3
	P8				C	S			S	S								S		1	4
	PG	S	S	S	S	C	S	S	S	S	S	S	S	S	S	S	S	S	C	2	16

C ->Vinculación clave "el riesgo está ligado directamente con el proceso"

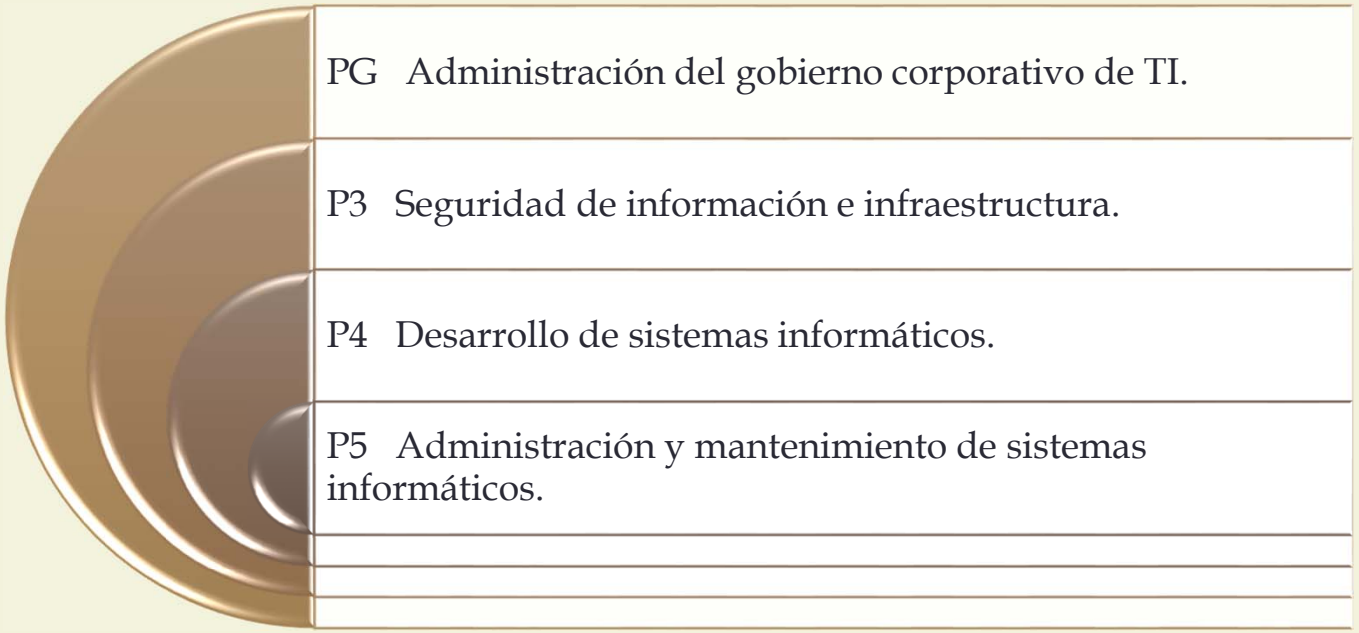
S ->Vinculación secundaria "el riesgo no afecta de forma directa al proceso"

Evaluación Técnica

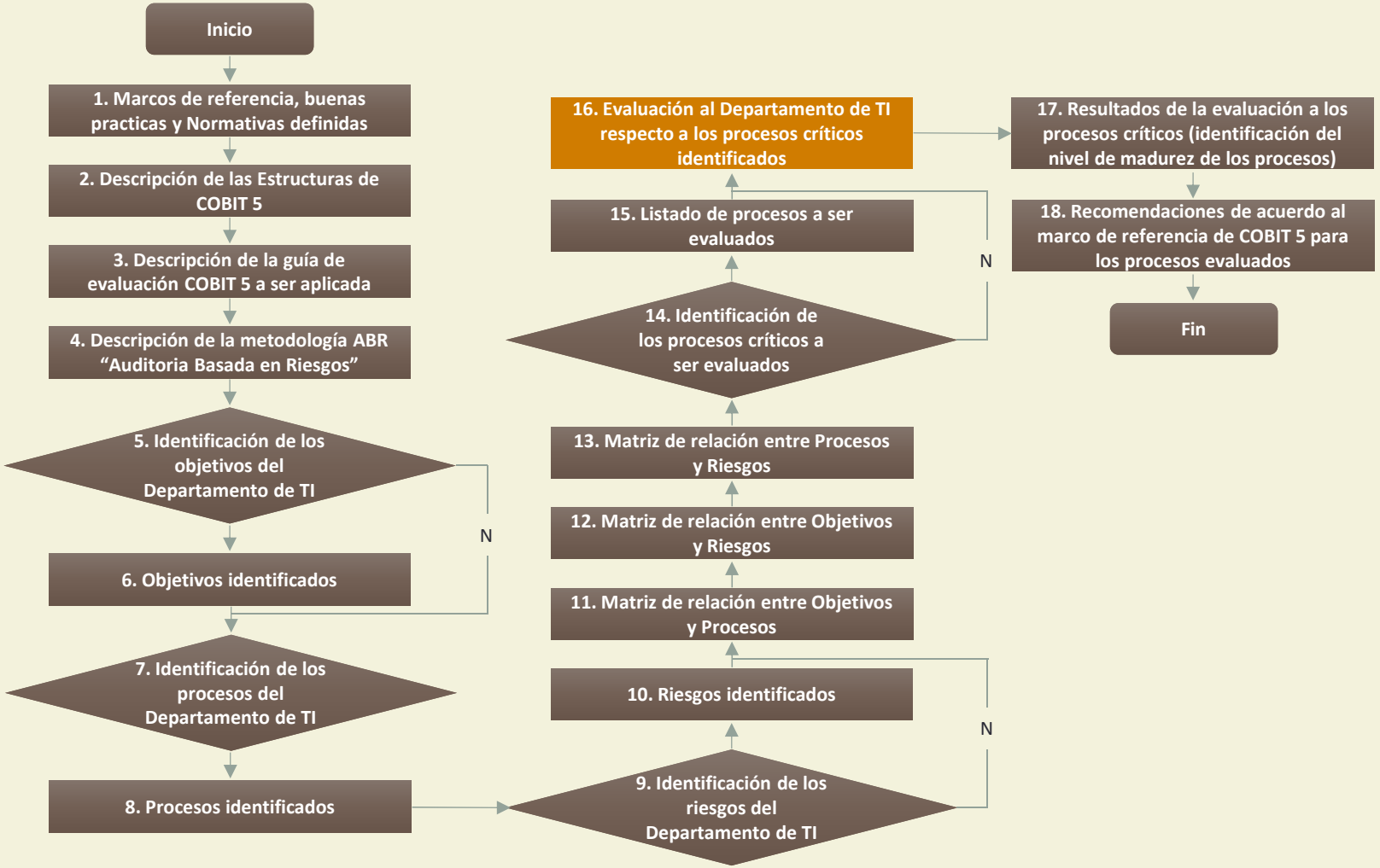


14. Identificación de los procesos críticos a ser evaluados

De acuerdo a la matriz de relación entre Procesos y Riesgos, se identifican los procesos críticos:



Evaluación Técnica



16. Evaluación al Departamento de TI respecto a los procesos críticos identificados

PROCESOS DE COBIT / PROCESOS DE TI	EDM 01	EDM 02	EDM 03	EDM 04	EDM 05	APO 01	APO 02	APO 03	APO 04	APO 05	APO 06	APO 07	APO 08	APO 09	APO 10	APO 11	APO 12	APO 13
PG	X	X	X	X	X													
P3														X			X	X
P4							X		X									
P5												X		X				

PROCESOS DE COBIT / PROCESOS DE TI	BAI 01	BAI 02	BAI 03	BAI 04	BAI 05	BAI 06	BAI 07	BAI 08	BAI 09	BAI 10	DSS 01	DSS 02	DSS 03	DSS 04	DSS 05	DSS 06	MEA 01	MEA 02
PG																		
P3									X			X		X	X			X
P4	X	X	X			X	X			X								
P5											X	X	X	X	X	X		

16. Evaluación al Departamento de TI respecto a los procesos críticos identificados

1. Encuesta al área del Departamento de Tecnología.

No.	Meta del Proceso	Preguntas	Respuesta	Promedio	Evidencias
1	EDM01-01	¿La presidencia, directivos, empleados en general están satisfechos con el trabajo realizados por TI?	5 / 5	5 / 5	Oficios y actas.
2	EDM01-01	¿Las decisiones de TI son claves y cumplen con los objetivos del organismo?	5 / 5		Documento PETI.
3	EDM01-02	¿Las funciones de TI están debidamente asignadas a los responsables para la correcta gestión de los procesos del organismo?	5 / 5	4 / 5	Documento de Roles y Funciones.
4	EDM01-02	¿Las funciones que cumple TI están evidenciadas en procesos y prácticas?	3 / 5		Documento de Directrices de TI y manuales de procesos.
5	EDM01-03	¿La dirección de TI cumple con enviar sus reportes de desempeño a los altos directivos del organismo?	5 / 5	5 / 5	Oficios.
6	EDM01-03	¿El directivo de TI se reúne con frecuencia con los altos directivos para revisar temas concernientes a TI?	5 / 5		Calendarización de reuniones.

16. Evaluación al Departamento de TI respecto a los procesos críticos identificados

2. Calificación de las Metas de cada Proceso de COBIT 5

Calificación	Criterio	
0 – 1.4	**N**	No logrado
1.5 – 3.4	**P**	Parcialmente logrado
3.5 – 4.4	**L**	Logrado gran parte
4.5 – 5	**F**	Totalmente logrado

16. Evaluación al Departamento de TI respecto a los procesos críticos identificados

3. Tabla de evaluación detallada.

EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno.					
Nivel	**Evaluar si se consiguen los siguientes resultados**	**Meta del proceso**	**No logrado (0-15%)**	**Parcialmente logrado (15% -50%)**	**Gran parte logrado (50% - 85%)**	**Totalmente logrado (85-100%)**
Nivel 0 Incompleto	El proceso no está implantado o falla en lograr su propósito.					
Nivel 1 Realizado	PA 1.1 Rendimiento del proceso.	EDM01-O1				**F**
		EDM01-O2			**L**	
		EDM01-O3				**F**
Nivel 2 Gestionado	PA 2.1 Gestión de rendimiento.					**F**
	PA 2.2 Gestión del producto de trabajo.					**F**
Nivel 3 Establecido	PA 3.1 Definición del proceso.					**F**
	PA 3.2 Despliegue del proceso.					**F**
Nivel 4 Predecible	PA 4.1 Medición de procesos.				**L**	
	PA 4.2 Control de Procesos.				**L**	
Nivel 5 Optimizado	PA 5.1 Innovación del Proceso.			**P**		
	PA 5.2 Proceso Optimizado.			**P**		

16. Evaluación al Departamento de TI respecto a los procesos críticos identificados

4. Tabla de evaluación resumida.

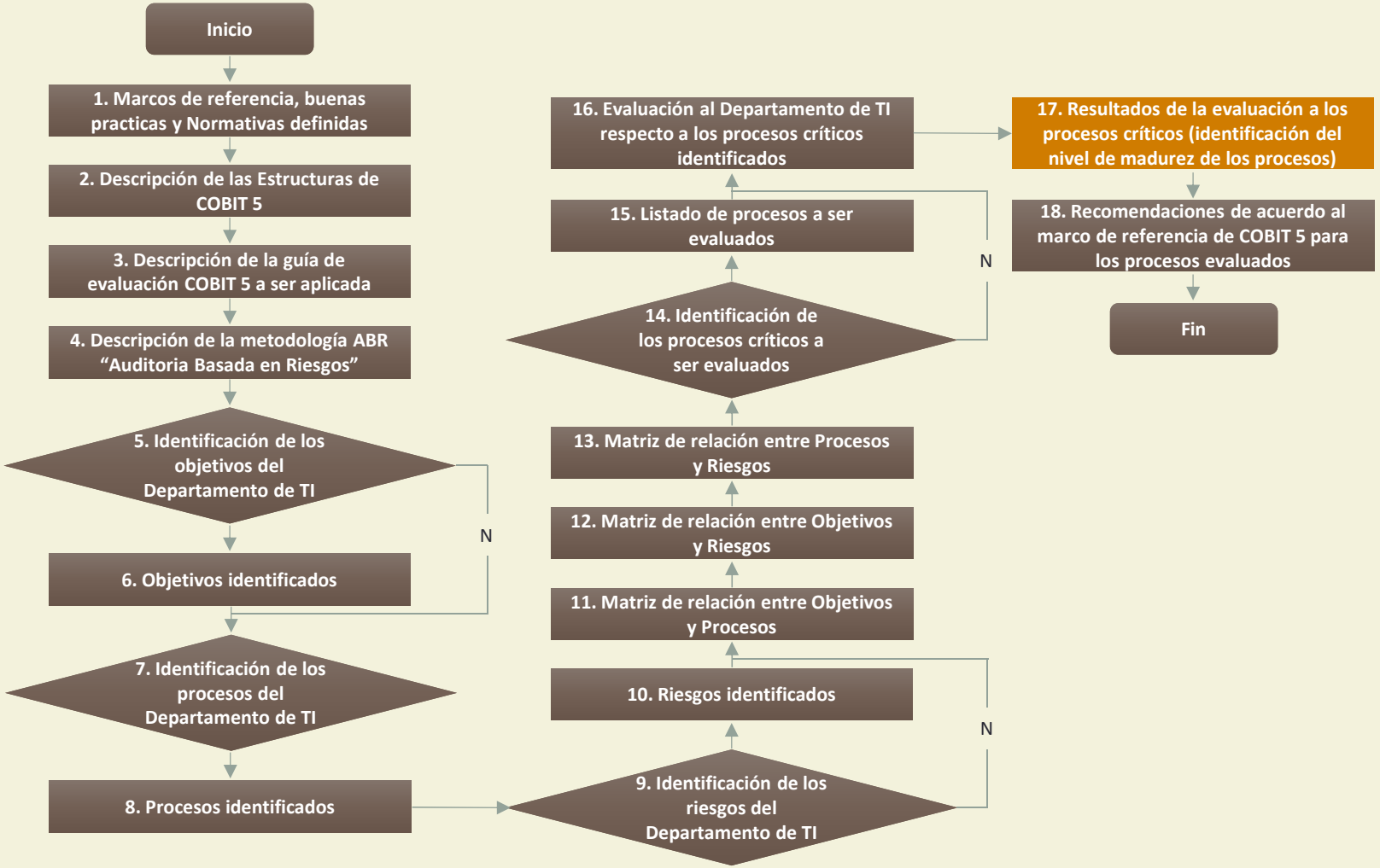
Nombre del Proceso	Nivel 0	Nivel 1	Nivel 2		Nivel 3		Nivel 4		Nivel 5	
EDM01		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA5.2
Criterio de Evaluación		F	F	F	F	F	L	L	P	P
Nivel de capacidad alcanzado								4		

16. Evaluación al Departamento de TI respecto a los procesos críticos identificados

5. Evidenciar el nivel de madurez.

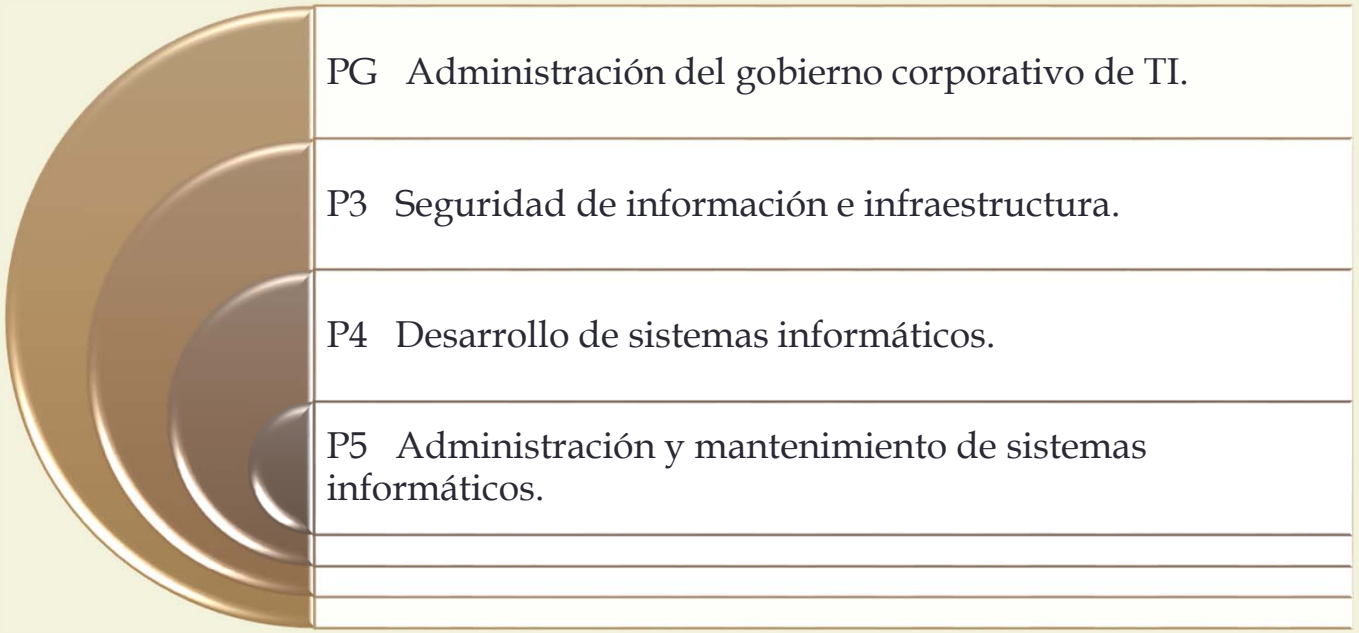
Nivel de Madurez	Nivel de capacidad
Nivel 0 Proceso Incompleto	
Nivel 1 Proceso Realizado	
Nivel 2 Proceso Gestionado	
Nivel 3 Proceso Establecido	
Nivel 4 Proceso Predecible	4
Nivel 5 Proceso Optimizado	

Evaluación Técnica



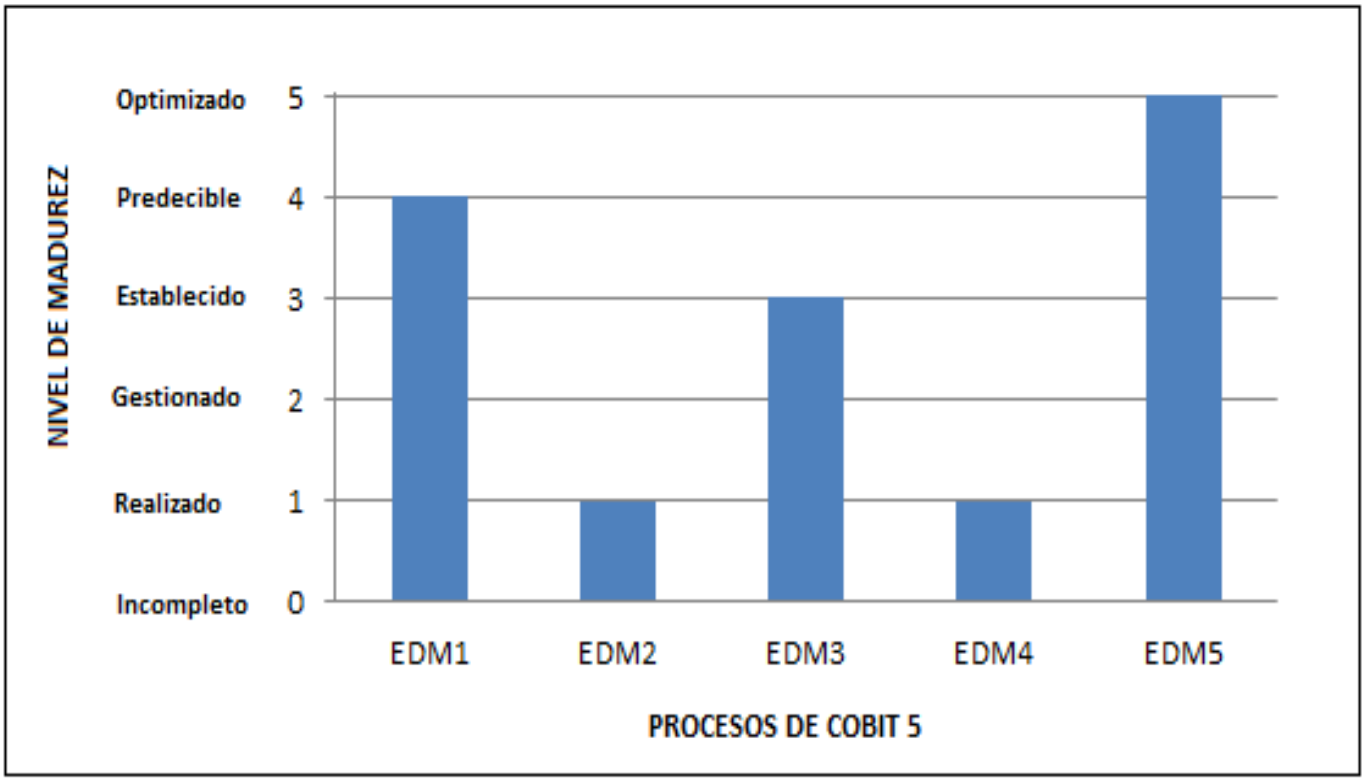
17. Resultados de la evaluación a los procesos críticos (identificación del nivel de madurez de los procesos)

Los cuatro procesos críticos del Departamento de Informática fueron evaluados mediante la metodología de COBIT v5 los cuales muestran los siguientes resultados:



Informe del PG Proceso Gobierno Corporativo de TI

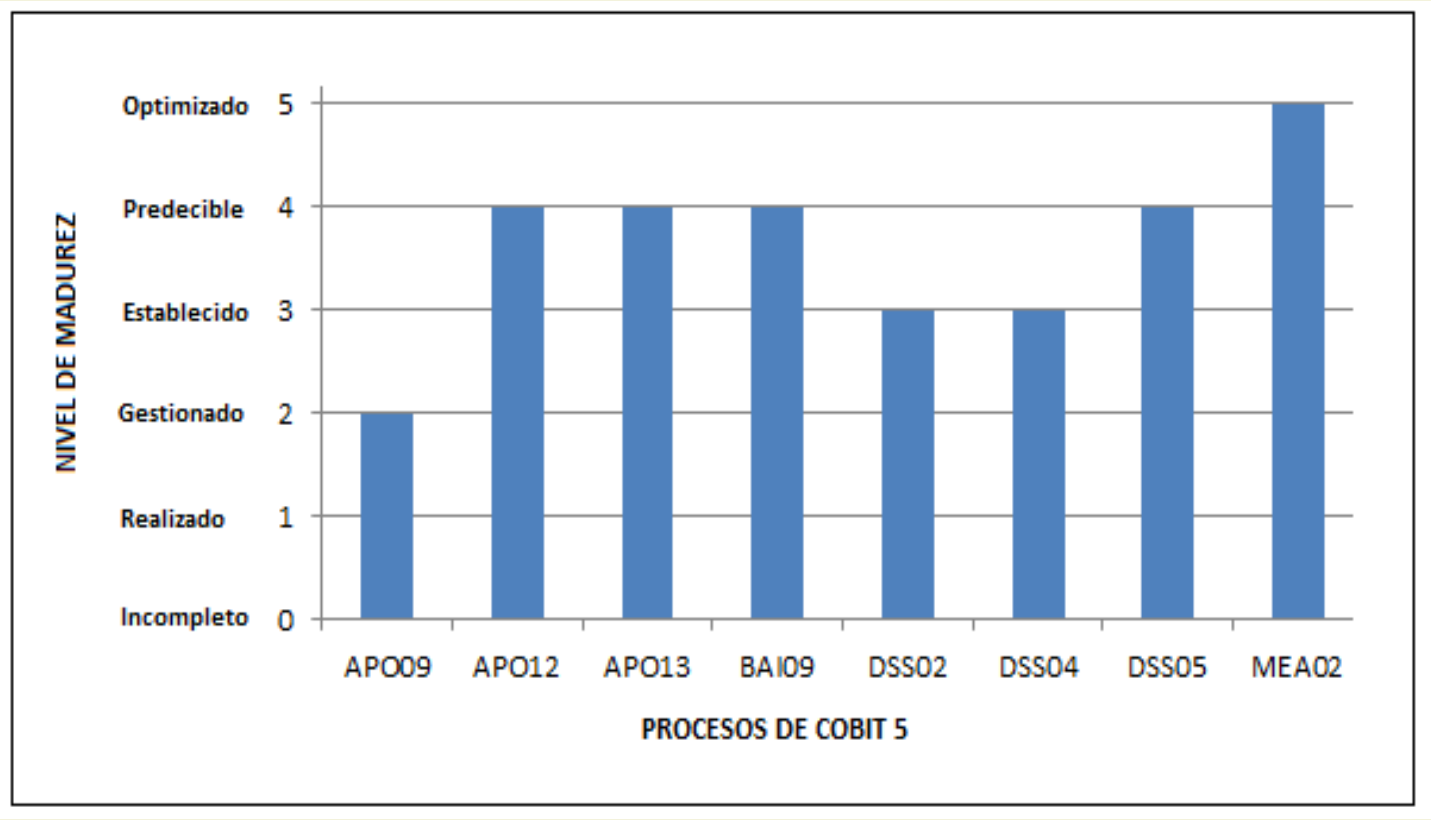
EDM01 Marco Gobierno TI	EDM02 Entrega de Beneficios	EDM03 Optimizar Riesgo	EDM04 Optimizar Recursos	EDM05 Transparencia hacia partes interesadas



Informe de la evaluación del Proceso P3 Seguridad Informática e Infraestructura

APO09 Acuerdos de Servicio | APO12 Gestionar Riesgo | APO13 Gestionar Seguridad | BAI09 Gestionar Activos | DSS02 Incidentes de Servicio

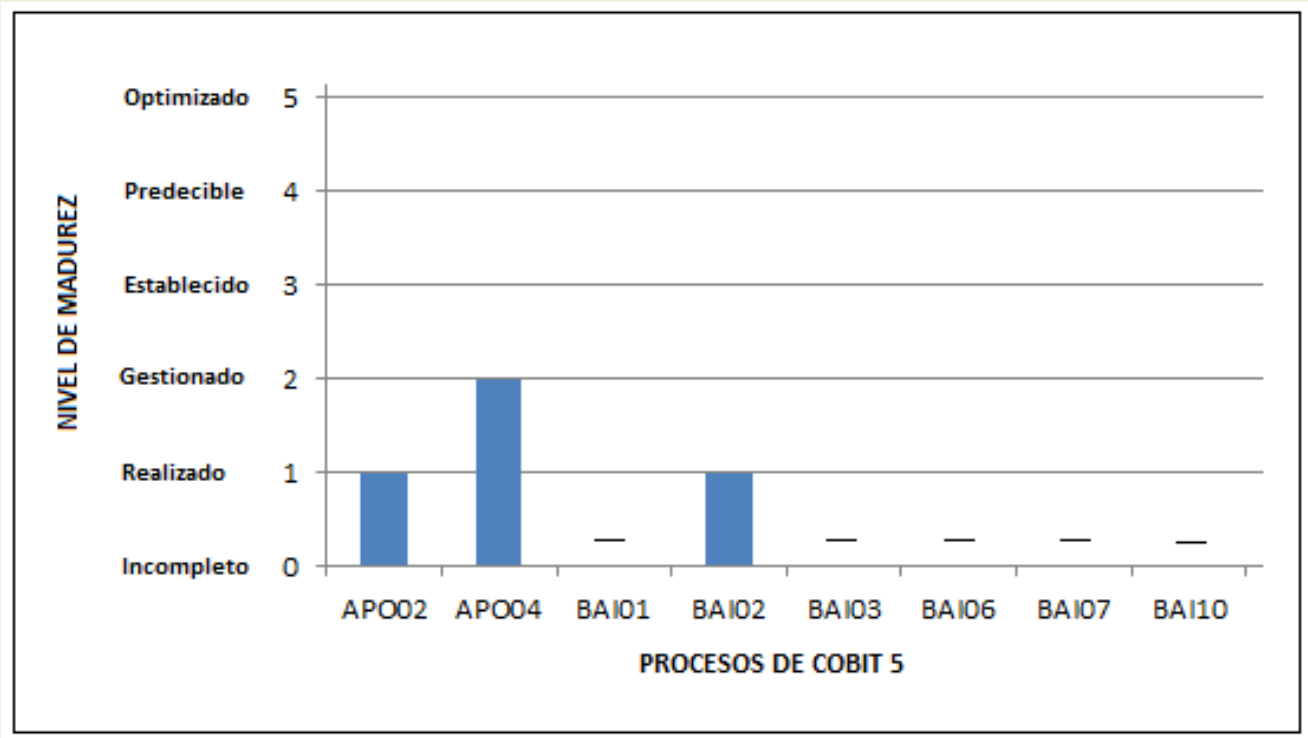
DSS04 Continuidad Servicio | DSS05 Servicios de Seguridad | MEA02 Control Interno



Informe de la evaluación del Proceso P4 Desarrollo de Sistemas Informáticos

APO02 Gestionar Estrategia | APO04 Gestionar Innovación | BAI01 Programas y Proyectos | BAI02 Definición de Requisitos | BAI03 Construcción de requisitos

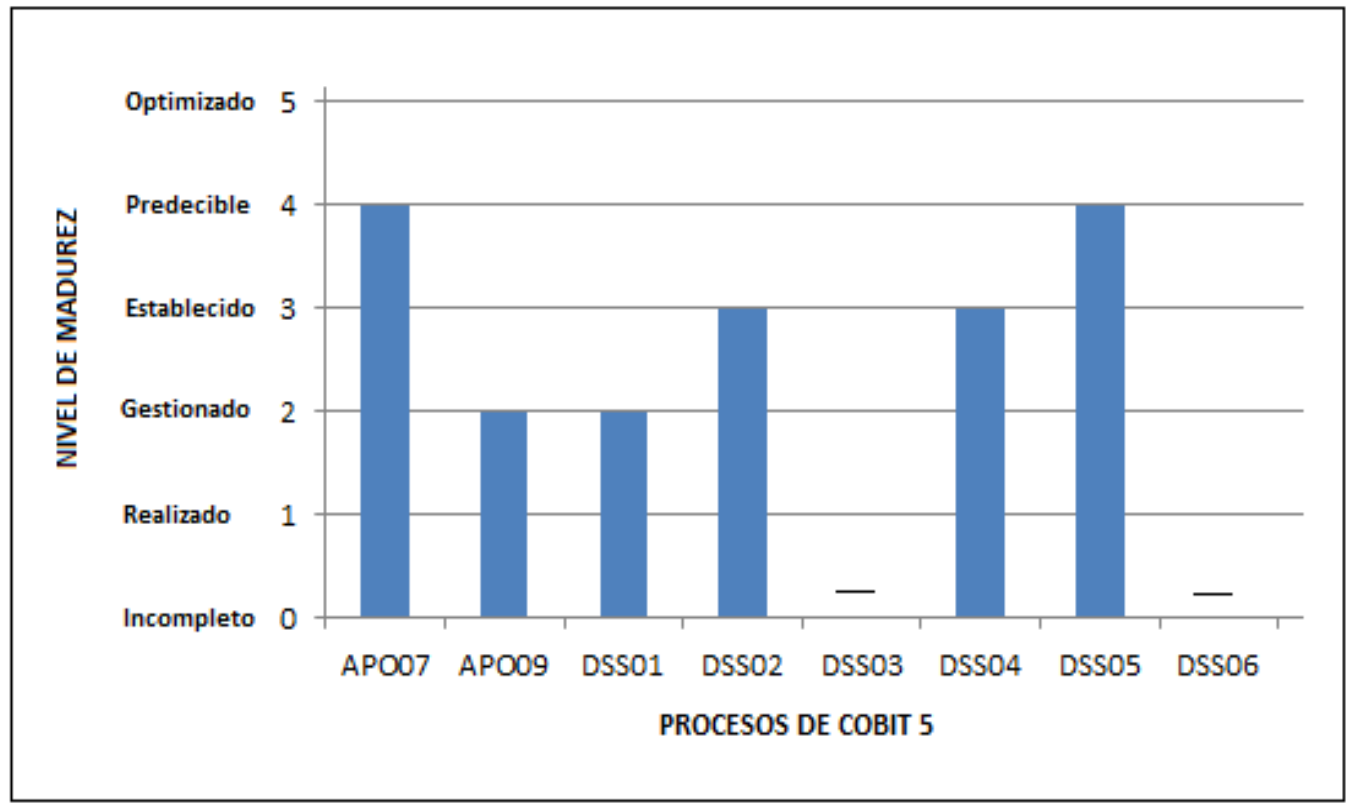
BAI06 Gestionar Cambios | BAI07 Aceptación cambio | BAI10 Gestionar Configuración



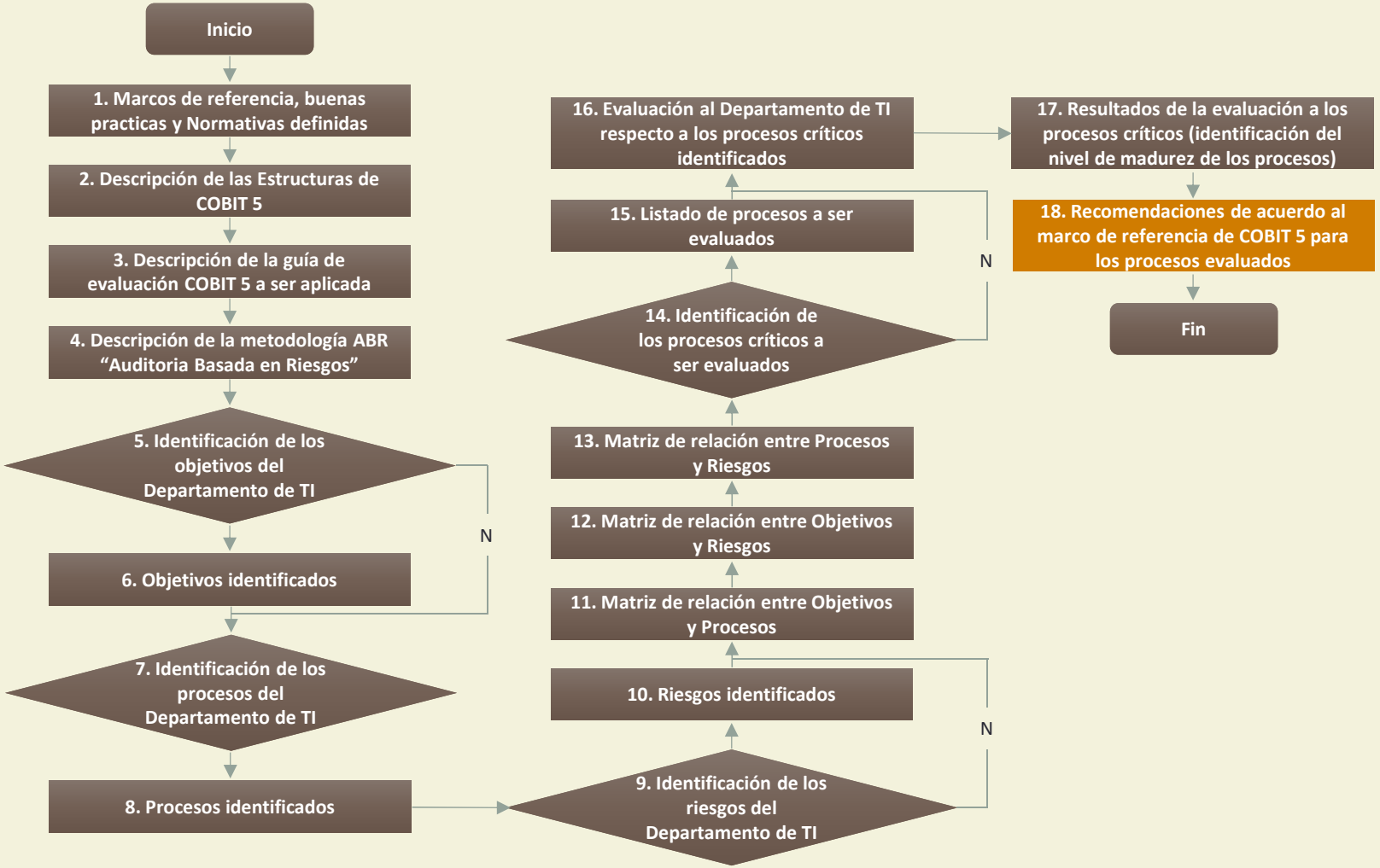
Informe de la evaluación del Proceso P5 Administración y Mantenimiento de Sistemas Informáticos

APO07 Recursos Humanos | APO09 Acuerdos de Servicio | DSS01 Gestionar las operaciones | DSS02 Incidentes de Servicio | DSS03 Gestionar Problemas

DSS04 Continuidad Servicio | DSS05 Servicios de Seguridad | DSS06 Controles de Procesos



Evaluación Técnica



18. Recomendaciones de acuerdo al marco de referencia de COBIT 5 para los procesos evaluados

- ✓ Medir persistentemente el desempeño del área de TI en términos de la institución y controlar los gastos de TI .
- ✓ Definir reglas y procedimientos de escalado de incidentes, especialmente para incidentes importantes e incidentes de seguridad.
- ✓ Llevar a cabo periódicamente evaluaciones de vulnerabilidades de seguridad lógica para determinar si los dispositivos de seguridad perimetral, bases de datos o servidores están seguros de intrusiones.
- ✓ Efectuar el Plan de Continuidad del Negocio BCP enfocados en los procesos críticos de la Institución.

18. Recomendaciones de acuerdo al marco de referencia de COBIT 5 para los procesos evaluados

- ✓ Utilizar peticiones de cambio formales para que los propietarios de procesos del organismo y TI soliciten cambios en procesos de negocio o aplicaciones; y asegurar que estos cambios estén controlados a través del proceso de gestión de cambios.
- ✓ Definir un plan de calidad (QA) para especificar procesos de validación y verificación, definición de cómo se revisará y calificará la calidad, y roles para la consecución de la calidad.
- ✓ Definir acuerdos de nivel operativo OLAs y de servicio SLAs para establecer normas y procedimientos de disponibilidad del servicio y responsables.
- ✓ Mantener un catálogo de gestión de problemas a ser registrados y determinar niveles de prioridad para dedicarse a la resolución de problemas basándose en los riesgos del organismo.

Conclusiones

- La evaluación técnica del Gobierno Corporativo de TI realizada mediante los procesos catalizadores EDM de COBIT v5 sirve como una referencia de oportunidades de mejora para una futura certificación ISO 38500 en la institución.

- Mediante el análisis de riesgos realizado se pudo determinar claramente cuáles son los procesos de tecnología críticos del organismo y cuyos riesgos deben ser tratados adecuadamente.

- Implementar directrices de Gobierno de TI dentro de la Institución es fundamental para que la alta gerencia considere a TI como una área importante y estratégica en la cual se debe invertir para cumplir con los objetivos y proyectos institucionales.

Recomendaciones Generales

- Crear el área estratégica de Gobierno de TI responsable de supervisar y asegurar la entrega de beneficios, uso de recursos tecnológicos y gestión de riesgos de manera eficiente.
- Reestructurar organizacionalmente el área de Seguridad Informática y colocarla en otra Dirección diferente a TI con el objeto de gestionar y evaluar los procesos de control de la información en las todas las funciones de TI.
- Implantar el área proyectos de TI para planificar, organizar y administrar el presupuesto y portafolio de programas y proyectos de TI.

GRACIAS