Operaciones Subcontratadas ISAE3 402 / SSAE18

2018

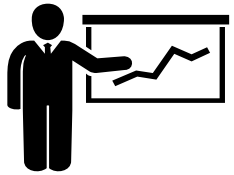
kpmg.com.co

Agenda

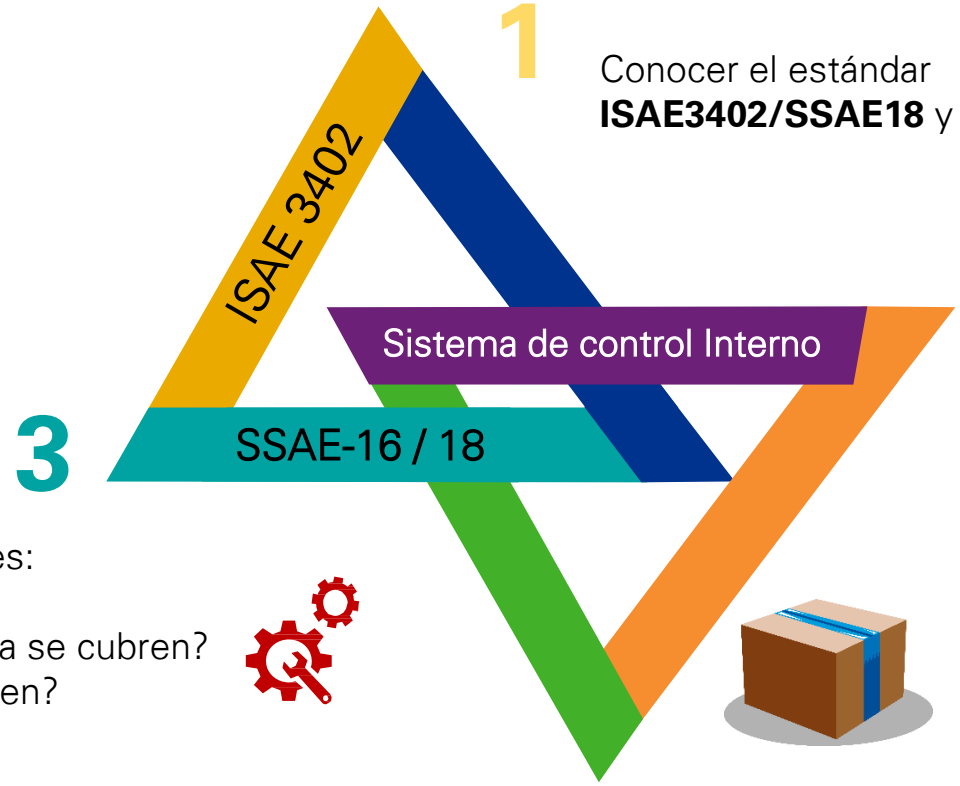
1. Objetivo y Alcance
2. Introducción
3. Que es ISAE 3402 / SSAE-18
4. SOC Tipos de Reportes
5. Componentes del informe SOC
6. Aspectos Relevantes a tener en cuenta
7. Cuales beneficios tengo
8. Que elementos se evalúan
9. Resultados e implicaciones de la evaluación
10. Resumen del ciclo IT Attestation / SOC
11. Que hacemos – Como puede KPMG ayudarle?

Objetivos

Dar a conocer la norma que rige los **lineamientos** para reportar sobre el control interno en las organizaciones de servicio y como afecta este, el ambiente de las Compañías u organizaciones Usuarias.



IT Attestation



1

Conocer el estándar **ISAE3402/SSAE18** y su alcance

2

Identificar la importancia, relevancia e implicación **que tiene el sistema de control interno preparado por las organizaciones de servicio para soportar los procesos y presentar, diseñar e implementar los controles,** para el soporte de la Operación y el procesamiento de información como fuente para la **generación y reporte de los estados financieros de las organizaciones usuarias (Compañías)**

3

Dar respuesta a los interrogantes:

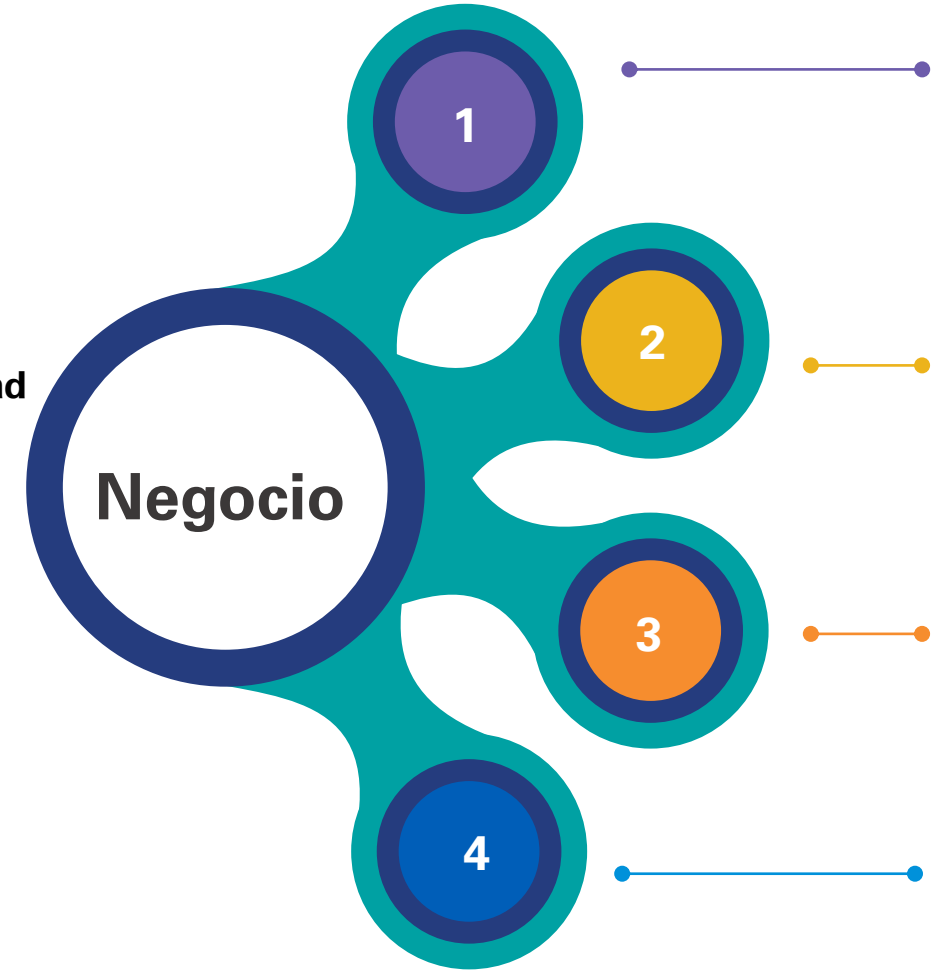
- ¿Qué **Necesidad** o Problema se cubren?
- ¿ Qué **Beneficios** se Obtienen?

Introducción

Bajo la norma internacional de trabajos para atestiguar ISAE, se encuentran ISAE 3402, SSAE-18, ISAE 3000.

IT Attestation

Existe una creciente **necesidad sobre el uso de servicios Tecerizados respecto a las funciones de negocio no misionales** de las compañías.



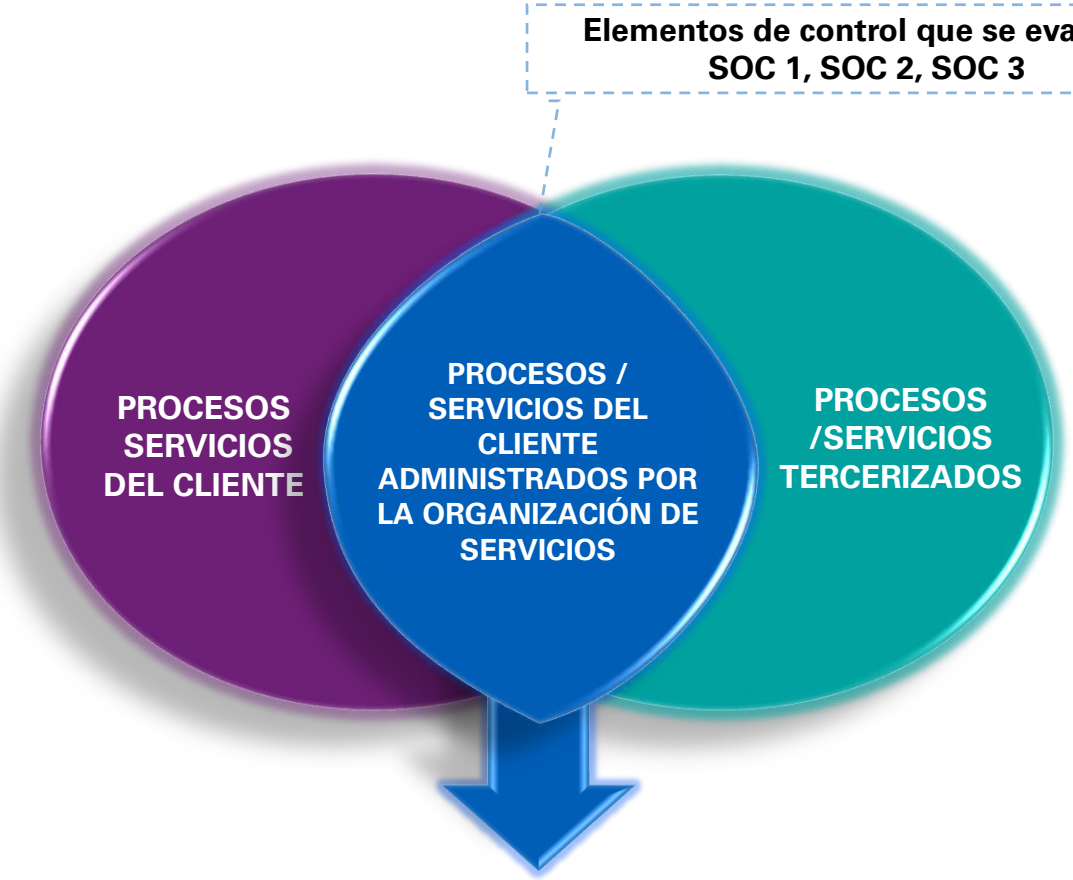
- Alta demanda del uso de servicios tercerizados asociados con a) el procesamiento de información, b) administración de la infraestructura, c) desarrollo de aplicaciones, d) Data Center, e) nomina y f) procesos de visación y canje, entre otros aspectos.
- Las compañías, incrementado **los procesos de aseguramiento, sobre actividades realizadas por sus organizaciones de servicios,** como complemento a la norma internacional de **Auditoria 402**
- Como respuesta a las diferentes amenazas emergentes, y el amplio **número de requerimientos regulatorios**.

Aspecto relevante: Las compañías siguen siendo responsables de **su ambiente de control**.

¿Qué es ISAE3402/SSAE18?

ISSAE 3402: ISAE (International Standards for Assurance Engagements) 3402 es un estándar de aseguramiento global para reportar sobre los controles de una organización que brinda **servicios tercerizados. Entró** en vigencia el **15 de junio** de 2011, básicamente en respuesta a la **Ley Sarbanes-Oxley**, para proteger a los accionistas y al público en general de **los errores contables y las prácticas fraudulentas**.

ISAE 3402 es una extensión y expansión de SAS 70 (the Statement on Auditing Standards No. 70), definió los estándares que un auditor debe emplear para **evaluar los controles internos contratados a una organización de servicios.**



ISAE3402 / SSAE18
(International Standards for Assurance Engagements)

SSAE18: A partir de la existencia del nuevo estándar internacional **ISAE 3402**, cada **país diseño su norma local para cumplir con los requerimientos específicos de sus legislaciones internas**. Este es el caso de los Estados Unidos, donde se creó el **SSAE 16** (Statement on Standards for Attestation Engagements 16), basado en el estándar internacional. El mismo se actualizó en mayo de 2017 a **SSAE18**.

Canadá, Reino Unido, chile. Colombia, Decreto 2132 del 22 / 12/2016.

SOC - Tipos de reporte (1/2)

*SOC: Service Organization Control

Informe de **Controles en una Organización de Servicios** que son relevantes para el Control Interno de las Entidades Usuarias sobre los Informes Financieros (ISAE 3402/SSAE 18)

En un Reporte **Tipo 1, e**l auditor de servicios manifestará su opinión sobre:

- La equidad en la **presentación** de la descripción que la administración efectúa sobre el sistema de la empresa de servicios durante el período
- La idoneidad del **diseño** de los controles en un punto determinado del tiempo.

Informe de Controles en una Organización de Servicios que son Relevantes para la Seguridad, Continuidad, Procesamiento, Integridad, Confidencialidad o Privacidad (AT101) (ISAE 3000)

Informe de Servicios de Confianza para Organizaciones de Servicios

En un Reporte **Tipo 2**, el auditor de servicios manifestará su opinión sobre:

- La equidad en la **presentación** de la descripción que la administración efectúa sobre el sistema de la empresa de servicios durante el período
- La idoneidad del **diseño** de los controles durante el período
- La **efectividad operativa** de los controles durante el período

SOC - Tipos de reporte (2/2)

Enfoque	Reporte	Resumen	Aplicación
Control Interno sobre Reporte Financiero	SOC 1 (*)	Reporte detallado para los usuarios y sus auditores	• Enfocado a riesgos y controles sobre **el reporte financiero especificados por el proveedor de servicios**. • Aplicable cuando el proveedor ejecuta el procesamiento de **transacciones financieras o soporta sistemas que procesan transacciones financieras**.
Controles Operacionales	SOC 2	Reporte detallado para los usuarios, sus auditores, y partes específicas	• Enfocado a: - Seguridad - Disponibilidad - Confidencialidad - Integridad del procesamiento - Privacidad
Controles Operacionales	SOC 3 (**)	Reporte corto que puede ser generalmente mayor distribuido, con la opción de desplegar un sello en el sitio web	Aplicable a una amplia diversidad de sistemas

Componentes del informe SOC

Sección I Informe de los auditores independientes **Reporte Tipo 1**

Sección II Declaración de la organización de servicios

Sección III Descripción del Sistema de Gestión de Servicios para ISAE3402/SSAE18

Sección IV Objetivos de control, controles relacionados y pruebas de diseño realizadas por el Auditor Externo

Sección I Informe de los auditores independientes **Reporte Tipo 2**

Sección II Declaración de la organización de servicios

Sección III Descripción del Sistema de Gestión de Servicios para ISAE3402/SSAE18

Sección IV Objetivos de control, controles relacionados, pruebas de diseño y eficacia operativa realizadas por el Auditor Externo

Sección V Otra Información Proporcionada por la Organización de Servicios

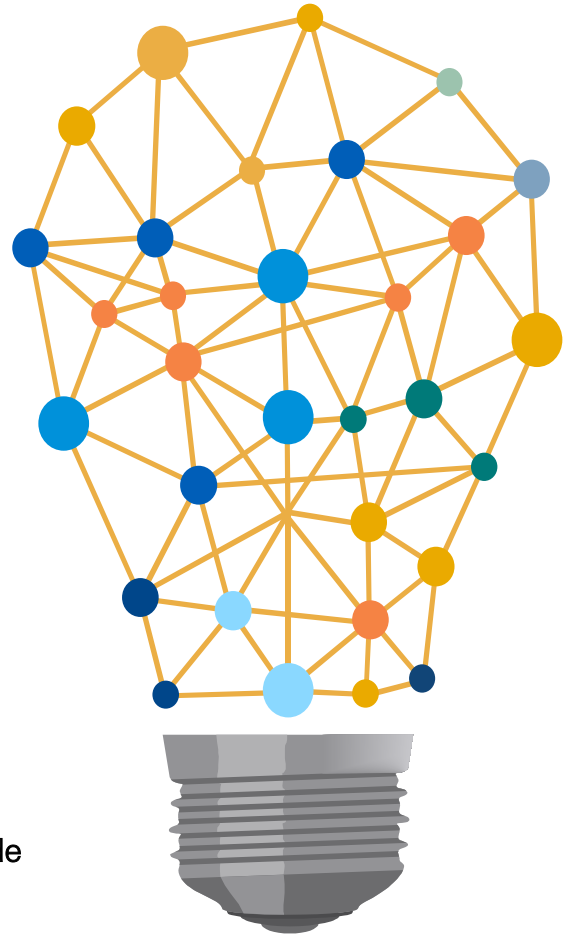
Aspectos Relevantes a tener en cuenta

01 ISAE 3402/SSAE18 refiere las responsabilidades de la Organización de Servicios al definir los objetivos y la descripción de controles para asegurar el ambiente de control preparado.

02 La Organización de servicios se expresa respecto a la presentación, diseño y eficacia operativa de sus operaciones; es decir, el Representante Legal de la Organización de Servicios confirma con su propia opinión que estas tres características aseguran razonablemente el logro de los objetivos de control identificados

03 El Representante Legal de la Organización de servicios debe tener bases sobre las cuales realiza esta aseveración y el auditor externo (KPMG), entra a verificar. Por este motivo, se realizan las pruebas de presentación, diseño, implementación y eficacia operativa de los controles que se han declarado para prestar el servicio.

04 La Identificación de riesgos por parte de la Organización de Servicios y la Generación de la carta de representación donde el Representante Legal de confirma que el ambiente preparado para prestar el servicio, no tendrá ningún efecto adverso en el sistema de control interno de su organización Usuaria.



05 El Auditor de la Organización de servicio, determina el efecto que tiene una organización de servicio en las aseveraciones de los estados financieros y su impacto frente al resultado de su cliente (organización usuaria).

06 Se verifica, si el reporte de la organización de servicio es el adecuado y refiere un ISAE3402 o el SSAE18.

07 Se valida si el alcance del nuevo reporte cubrirá todos los aspectos relevantes para los estados financieros.

08 Se asegura que el reporte de la organización de servicios sea del Tipo II, ya que para cubrir los aspectos relevantes de estados financieros debe contemplarse la aseveración de efectividad operativa.

¿Cuáles beneficios obtengo?

SOC	Descripción	Beneficios
SOC 1/2 TIPO	• SOC 1 Informe sobre los controles en una organización de servicios relevante para el Reporte Financiero • SOC 2 Informe sobre los controles en una organización de ser… ro… …a …sistema de una organización de servicios y la idoneidad del diseño de los controles.	• El reporte SOC 1 esta enfocado a riesgos y controles sobre el reporte financiero especificados por el proveedor de servicios.
SOC 1/2 TIPO	O… er… O… servicio relevante para seguridad, disponibilidad, procesamiento de integridad, confidencialidad o privacidad. …a …st… …is… • El uso de estos informes está restringido.	…información, un mecanismo para evaluar el gobierno y supervisar… esos proveedores de servicio.
SOC 3	• Reporte corto que puede ser generalmente mayor distribuido, con la opción de desplegar un sello en el sitio web • Uso no restringido y capacidad para desplegar un sello en el sitio web.	respecto a las áreas operacionales de interés para los clientes o entidades usuarias. • El reporte SOC 2 o SOC 3 puede aprovechar los controles existentes en SOC1 a fin de alcanzar los principios y criterios de Trust Services de la AICPA para emitir un reporte SOC 2 y/o SOC 3 en conjunto con el actual reporte SOC1.

01 Se abordan requerimientos del cliente para dar **cumplimiento** a las normas locales e internacionales. Ejm. **SOX – "Sarbanes Oxley"**

02 Provee a las organizaciones usuarias un nivel de **seguridad razonable** de la **integridad** y **efectividad** de los controles establecidos en los diversos procesos de negocio y de tecnología de información que se han **tercerizado**.

03 Provee a las organizaciones usuarias un nivel de **seguridad razonable** de la **integridad** y **efectividad** de los controles establecidos en los diversos procesos de negocio y de tecnología de información que se han **tercerizado**.

¿Qué elementos se evalúan? (1/2)

- **Aseveración:** Se validarán las bases sobre las cuales la Organización de Servicios emitirá su propia opinión sobre la **presentación, diseño** e **implementación** de los **controles** para el cumplimiento de sus objetivos.
- **Presentación:** La descripción de los controles presenta razonablemente, en todos los aspectos importantes, los controles de la Organización de Servicios que puedan ser **relevantes** al control interno de sus organizaciones usuarias, en lo que se refiere a una evaluación asociada a los procesos de **Operación** y **Tecnología** de Información.
- **Diseño:** El conjunto de controles están debidamente diseñados para proporcionar un aseguramiento razonable que los **Objetivos de Control** serán logrados.
- **Implementación:** Estos controles se han puesto en **funcionamiento** en el día especificado
- **Eficacia:** Los controles que seleccionemos para probar están **operando** con eficacia suficiente para proporcionar un grado razonable que indique que los objetivos de control se lograron durante el periodo especificado. (Aplica únicamente para el **SOC 1 Tipo II**).

¿Qué elementos se evalúan? (2/2)

01	Identificación y **calificación** del **Riesgo**
02	La definición del **objetivo** de Control y el grupo de **controles** con el cual se logra el objetivo
03	✓ **Diseño** del Control: **qué, quién, cuando, cómo** y **evidencia** que se deja de la ejecución del control. ✓ **Eficacia** operativa del Control: **evidencia** de la **ejecución** del control en el **periodo** objeto de evaluación

Ambiente de control del servicio

Resultados e Implicaciones de la Evaluación

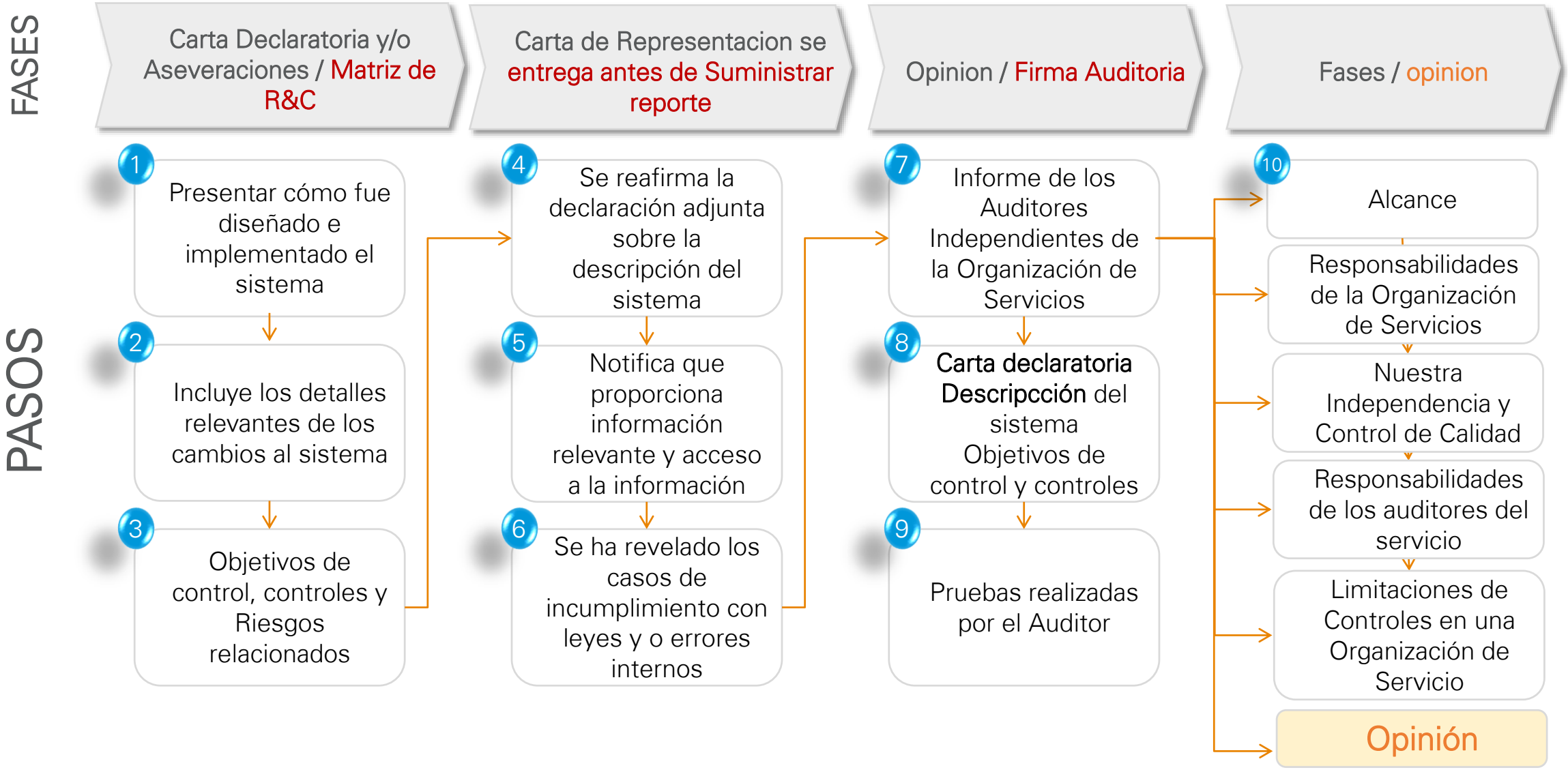
01

✓ **Opinión Sin Salvedad** : la opinión informa que los controles están **diseñados adecuadamente,** para proporcionar una seguridad razonable de que se lograron los objetivos de control establecidos en la descripción de la organización de servicios, de su sistema, y que los estos **operaron eficazmente**.

02

✓ **Opinión Con Salvedad (calificada)**: la opinión informa que los controles **no están diseñados** adecuadamente para proporcionar una seguridad razonable de que se lograron los objetivos de control establecidos en la descripción de la empresa u organización de servicios, de su sistema y que los controles **no operaron eficazmente.**

Resumen del ciclo IT Attestation / SOC



Sesión de Preguntas ¿?

Gracias.

The contacts at KPMG in connection with this report are:

Fabian Echeverria

Socio
KPMG Advisory, Tax & Legal SAS

Tel: +57 (1) 618-8000
Fax: +57 (1) 623-3380
fecheverria@kpmg.com

Constanza Consuelo Torres

Manager, Bogotá
KPMG Advisory, Tax & Legal SAS

Tel: +57 (1) 618-8000
Fax: +57 (1) 623-3380
cctorres@kpmg.com