


## CONTENIDO

1.	OBJETIVO.....	2
2.	ALCANCE.....	2
3.	DEFINICIONES.....	2
4.	NORMATIVIDAD EXTERNA APLICABLE.....	8
5.	MARCO DE REFERENCIA DE EVALUACIÓN DEL CONTROL INTERNO SOBRE REPORTE FINANCIERO .....	9
6.	MODELO DE CUMPLIMIENTO SOX.....	11
7.	ORGANIGRAMA DE RESPONSABILIDAD FRENTE LA POLITICA.....	13
8.	MODELO DE LAS TRES LINEAS DE DEFENSA.....	13
9.	ROLES Y RESPONSABILIDADES PARA EL CUMPLIMIENTO SOX.....	14
10.	ENFOQUE SOX.....	19
11.	IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS.....	21
12.	ACTIVIDADES DE CONTROL.....	27
13.	EVALUACIÓN DE CONTROLES.....	47
14.	INFORMACIÓN Y COMUNICACIÓN.....	52
15.	DOCUMENTOS DE REFERENCIA.....	54
16.	CONTROL DE CAMBIOS.....	54
17.	FIRMAS DE REVISIÓN Y APROBACIÓN.....	55

	<p style="text-align: center;">POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</p>	Página 2 de 55
		Versión: 02
		Fecha: 01/06/2020

## 1. OBJETIVO

Establecer los lineamientos para el cumplimiento de la Ley Sarbanes Oxley (SOX), con el fin de asegurar que se mitiguen los riesgos de fraude o error material en los estados financieros.

## 2. ALCANCE

La presente política está dirigida y será aplicable a los miembros de la Alta Dirección y Colaboradores de Proindesa S.A.S. y sus sociedades administradas (vehículos de inversión en infraestructura vial bajo alcance SOX definido por Grupo Aval)<sup>1</sup>, en adelante “La Organización”.

La aplicación de esta Política es responsabilidad del Oficial SOX de Proindesa S.A.S. de acuerdo con las directrices emitidas por Grupo Aval.

Esta Política hace parte del Sistema de Administración de Riesgos de la Organización. y otras disposiciones de carácter interno, entre las que se encuentran: el Código de Ética y Conducta, el Sistema de Administración de Riesgo Operativo (SARO), el Sistema de Gestión del Riesgo Anticorrupción y el Sistema de Gestión de Seguridad de la Información (SGSI).

## 3. DEFINICIONES

**Alcance SOX:** Planeación anual de las entidades y procesos relevantes que son objeto de aplicación de la metodología SOX. Abarca la siguiente clasificación:

- **Entidades con enfoque 1 o enfoque completo:** Entidades que por aspectos cualitativos (riesgo) y/o cuantitativos (materialidad de cuentas significativas) son considerados como clave. Presentan más de una cuenta contable superior a la materialidad, por lo tanto, tienen más de un proceso bajo alcance, lo cual implica que incluye los procesos de: Controles a Nivel de Entidad, Controles Generales de Tecnología de Información, Contable y Consolidación, Migración y Adquisición de Negocios.

<sup>1</sup> En virtud del Acuerdo de Colaboración Empresarial suscrito entre Proindesa S.A.S. estas sociedades.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

Código: DG-0106/2

- **Entidades con enfoque 2 o enfoque particular:** Entidades que, aunque tienen algunas cuentas contables superiores a la materialidad de cuentas significativas, su nivel de riesgo derivado de la evaluación cualitativa es relativamente bajo. Normalmente, estas entidades tienen una sola cuenta superior a la materialidad y, por lo tanto solo tienen un proceso alcanzado.
- **Otras entidades:** Corresponden a las demás entidades que deberán mantener un sistema de control interno sobre reporte financiero apropiado, que le permita a la administración tener la certeza sobre la razonabilidad del reporte financiero.

**Alta dirección:** Junta Directiva, Presidente, Representante Legal, Vicepresidentes de Proindesa S.A.S. o quienes hagan sus veces en la organización.


**Ambiente de control:** Es la base de los componentes del Sistema de Control Interno, define los principios y el gobierno con los cuales se rige la Organización e influye en los colaboradores sobre la forma en que se deben llevar a cabo las operaciones.

**Aplicación administrativa:** Soportan controles asociados a los procesos de ELC (Controles a Nivel de Entidad por sus siglas en inglés) e ITGC's (Controles Generales de Tecnología de Información por sus siglas en inglés) y que apoyan de forma indirecta el reporte financiero, por lo tanto, se excluyen del alcance SOX.

**Aplicación clave SOX:** Soportan controles de proceso del negocio, directamente relacionadas con el control interno sobre reporte financiero y hacen parte del inventario de aplicaciones SOX alcanzadas.

**Aplicaciones desarrolladas por el usuario (ADUs):** Consisten en hojas de cálculo y bases de datos creadas y utilizadas por los dueños de proceso o usuarios finales de la información para extraer, organizar, calcular y/o procesar datos para analizar tendencias, tomar decisiones o resumir datos financieros y reportar resultados. Las ADUs no están administradas ni desarrolladas en un ambiente de tecnología tradicional y no siguen un proceso de desarrollo formal, por tanto, no están cubiertas por los Controles Generales de Tecnología. Algunos ejemplos son: Hojas de cálculo (Excel), bases de datos (Access), consultas a bases de datos, scripts.

**Aseguramiento razonable:** Corresponde al entendimiento de que la probabilidad de que exista un error material que no se pueda prevenir o detectar oportunamente es remota. Debido a que la evaluación

	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 4 de 55
		Versión: 02
		Fecha: 01/06/2020

de la administración se realiza con base en muestras, el aseguramiento absoluto no es posible.

**Aserciones de los estados financieros:** Representaciones realizadas por la Alta Dirección, incluidas en las cuentas y subcuentas de los estados financieros. Pueden clasificarse en integridad, existencia, exactitud, valuación, derechos y obligaciones, presentación y revelación.

**Base de datos:** Conjunto de datos relacionados entre sí, que se almacenan de manera organizada para facilitar el acceso, gestión y actualización de estos, de manera rápida y estructurada.

**Cargos críticos o relevantes sobre el reporte financiero externo (SOX):** Colaboradores que tengan bajo su responsabilidad la ejecución de controles considerados como clave, así como su jefe directo y el Director, Gerente o Vicepresidente responsable del área respectiva (incluye cargos backup).

**Centros de Servicios Compartidos – CSC:** Aquella subordinada de Grupo Aval a la cual se le ha tercerizado algún proceso clave con impacto en SOX, es decir que presta servicios a otras entidades incluyendo Subordinadas de Grupo Aval, que tienen algún impacto en SOX. En este contexto, una entidad usuaria es aquella subordinada de Grupo Aval a la cual el Centro de Servicios Compartidos presta sus servicios.


**Colaboradores:** Trabajadores, incluyendo la Alta Dirección, estudiantes en práctica y aprendices de Proindesa S.A.S.

**Controles:** Actividades realizadas sobre el inicio, registro, procesamiento, monitoreo y reporte de las transacciones, que están diseñados para prevenir o detectar y corregir oportunamente errores en los estados financieros y mitigar los riesgos identificados en los procesos.

**Control interno:** Lo conforman el grupo de procedimientos diseñados, implementados o mantenidos por los colaboradores responsables del gobierno y administración de la organización, y por otras personas que suministran razonable aseguramiento sobre el logro de los objetivos de esta, relacionados con la confiabilidad de los reportes financieros, la efectividad y eficiencia de las operaciones y el cumplimiento con las leyes y regulaciones aplicables.

**Control interno sobre reporte financiero:** Comprende un proceso diseñado y/o supervisado por los principales ejecutivos de la Organización o las personas que realizan funciones similares, encargados

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 5 de 55
		Versión: 02
		Fecha: 01/06/2020

de suministrar un aseguramiento razonable en relación con la confiabilidad de los estados financieros de acuerdo con los principios contables generalmente aceptados.

**Controles clave:** Son aquellos que operan a un nivel de precisión que les permite cumplir con los objetivos para los cuales fueron establecidos, generalmente suministran la evidencia más completa y eficiente sobre las manifestaciones de los estados financieros para una o más cuentas significativas o revelaciones y mitigan de manera significativa la exposición al riesgo de error en los estados financieros.

**Controles compensatorios:** Son aquellos que operan a un nivel de precisión menor que el de un control clave pero que mitigan la posibilidad de que exista una exposición a un riesgo cuando otro control es deficiente. Si los controles preventivos operan efectivamente, estos pueden prevenir o detectar errores en los estados financieros.

**Controles complementarios:** Son aquellos que funcionan en conjunto con otros controles para cumplir con el mismo objetivo de control. Una falla en estos controles puede causar que no se cumpla con el objetivo del control o que se cumpla en un nivel diferente de precisión.

**COSO:** Marco de referencia de control interno. En 1992 el "Committee of Sponsoring Organizations (COSO)" publicó este marco de control, definiendo cinco componentes interrelacionados que deberán ser aplicados en cualquier nivel de la organización. Este marco fue actualizado en el año 2013, por lo cual es conocido como COSO 2013. Cuenta con cinco componentes que son ambiente de control, evaluación del riesgo, actividades de control, información y comunicación, y actividades de monitoreo, y 17 principios aplicables en toda la organización.

**Cuenta o revelación significativa:** Una cuenta o revelación es significativa si existe una posibilidad razonable de que la cuenta o revelación, contengan un error material que, individualmente o de manera agregada con otros errores, tengan un efecto material en los estados financieros, considerando tanto los riesgos de sobreestimación como de subestimación de dichos estados financieros. La determinación de si una cuenta o revelación significativa se basa en el riesgo inherente, antes de considerar el efecto de los controles.

**Deficiencia de Control:** Ausencia o insuficiencia en el diseño u operación de un control, que no permite a la gerencia o a los colaboradores detectar o prevenir errores en los estados financieros de manera oportuna durante el normal desarrollo de sus funciones.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

**Debilidad Material:** Es una deficiencia o combinación de deficiencias de control interno que indican la existencia de una “posibilidad razonable” de que un error en los estados financieros, por encima de o muy cercano a nivel de materialidad, no sea prevenido o detectado, afectando adversamente la habilidad para iniciar, autorizar, contabilizar, procesar o reportar la información financiera.

**Debilidad Significativa:** Es una deficiencia o combinación de deficiencias de control interno que indican la existencia de una “posibilidad razonable” de que un error en los estados financieros, que esté por debajo del nivel de materialidad, no sea prevenido o detectado, afectando adversamente la habilidad para iniciar, autorizar, contabilizar, procesar o reportar información financiera.


**Dueño de proceso / controles:** Hace referencia al grupo de personas que en conjunto se encargan de ejecutar y monitorear que se ejecuten los controles, tal y como fueron diseñados, de manera que la responsabilidad del dueño de proceso / controles es del área en sí y no solo del colaborador, jefe, Director, Gerente o Vicepresidente de área. Este último es el responsable de asegurar que, en su área, los controles sean ejecutados y monitoreados y que sobre estas actividades, se deje evidencia suficiente

**Entidades o sociedades Administradas:** Corresponde a los vehículos de inversión de infraestructura, a los cuales Proindesa S.A.S. les realiza la prestación de servicios en las áreas de: sistemas y operaciones, recursos humanos, administración y gestión de riesgos, contraloría, inversiones, jurídica, financiera y contable, conforme a los acuerdos de colaboración empresarial suscritos con dichas entidades.

**Inventario de Riesgos Genéricos:** Listado de riesgos emitido por Grupo Aval, que, a nivel de proceso relaciona los riesgos vigentes, aserciones y transacciones, indica los riesgos que tienen impacto en el reporte de la información financiera.

**Error:** Acción sin intención que puede generarse en una mala clasificación, valoración, presentación o revelación de la información financiera.

**Ley SOX:** Ley norteamericana emitida en el año 2002, aplicable para todas las empresas que cotizan en la Bolsa de Valores de Estados Unidos. Busca proteger a los inversionistas, a partir de la estructuración de un marco de requerimientos enfocados en incrementar el nivel de confiabilidad de la información financiera.

	<p style="text-align: center;">POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</p>	Página 7 de 55
		Versión: 02
		Fecha: 01/06/2020

**Materialidad:** Es la magnitud de una omisión o error de la información contable que puede cambiar o influir sobre el juicio de los usuarios de los estados financieros.

**Naturaleza del Control:** Un control puede ser manual (cuando es ejecutado por un funcionario) o automático (cuando requiere de un soporte tecnológico para su ejecución).

**Opción crítica SOX:** Transacción dentro de un módulo y aplicación SOX, con la cual se registra, procesa, y/o autoriza información que afecta el reporte financiero.

**Organización Prestadora de Servicios (OPS):** Entidad externa (o el segmento de una entidad) que suministra servicios a la Organización en relación con un proceso significativo en el cual dicha entidad realiza el inicio, contabilización, procesamiento y/o reporte de las transacciones o información con las cuales se generan los reportes financieros.

**Órganos de Control:** Corresponde a los órganos internos y externos de control, tales como la Auditoría Interna, Contraloría Corporativa de CFC, Comité de Auditoría o la Revisoría Fiscal.

**Periodicidad del Control:** Frecuencia en la cual se ejecuta el control, puede ser diaria, múltiples veces al día, semanal, quincenal, mensual, trimestral, semestral, anual, eventual o permanente.


**Pruebas de Controles:** Procedimientos de auditoría diseñados para evaluar la efectividad operativa de los controles definidos para prevenir o detectar y corregir errores materiales a nivel de manifestaciones (Aserciones / Aseveraciones).

**Reporte de Deficiencias de Control:** Herramienta que asiste a la administración para evaluar la importancia de las deficiencias de control interno de manera individual y agregada, para determinar si constituyen deficiencias significativas o debilidades materiales, e identificar temas y tendencias comunes a dos o más deficiencias, para propósitos de agregación.

**Reporte ISAE 3402 (Norma Internacional) o SSAE 16 (Norma Americana) Tipo II:** Es un informe de auditoría sobre una organización prestadora de servicios, que describe las políticas y procedimientos que son relevantes para el control interno de la organización usuaria (la que recibe el servicio), con el fin de determinar si dichas políticas y procedimientos fueron diseñados a la medida para lograr los objetivos de control, si estuvieron en operación al cierre de una fecha específica, si fueron probadas y

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código:** DG-0106/2

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 8 de 55
		Versión: 02
		Fecha: 01/06/2020

fueron efectivos para suministrar de una manera razonable, pero no absoluta, la seguridad de que se lograron los objetivos de control durante el período determinado.

**Riesgo:** Son eventos futuros inciertos, tanto positivos como negativos, que tienen el potencial de afectar el logro de las metas y objetivos de una compañía.

**Riesgo de control:** Posibilidad de que falle un control establecido en la organización y que ocurra un error material que no sea oportunamente prevenido o detectado. Debido a las limitaciones inherentes al control interno, siempre existirá un riesgo de falla de control.

**Riesgo de fraude:** Riesgo de error material sobre los estados financieros debido a la acción intencional cometida por un colaborador para asegurar una ganancia injusta o indebida.

**Security and Exchange Commission (SEC, por sus siglas en inglés):** Organismo del Gobierno Federal de Estados Unidos que ejerce supervisión sobre los participantes clave en el mercado de valores y cuya misión es proteger a los inversionistas, mantener el mercado de valores ordenado, eficiente y protegido contra el fraude, mantener información relevante sobre el mismo y facilitar la creación de capitales.

**Sistema operativo:** Software o programa que controla el orden y secuencia en la que se ejecutan las tareas del usuario y del sistema.

**Tablero de control:** mecanismo mediante el cual se realiza monitoreo a indicadores clave de desempeño (KPI) o indicadores clave de riesgo (KRI) para asegurar que las exposiciones residuales de riesgo se enmarcan en las políticas de apetito de riesgo, o si alguna exposición requiere monitoreo especial.

**Tolerancia:** Nivel aceptable de desviación del riesgo según el apetito definido, con relación a la consecución de los objetivos de negocio.

#### 4. NORMATIVIDAD EXTERNA APLICABLE

- **Ley Sarbanes Oxley:** Ley promulgada para proteger a los inversionistas a través del mejoramiento de la confiabilidad y exactitud de las revelaciones financieras, es conocida como

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------



Ley SOX.

- **Alert 11 del PCAOB:** comunicado mediante el cual el PCAOB recalca a los auditores externos y por consiguiente a sus auditados, la importancia de la evidencia suficiente para sustentar la certificación del auditor y de la administración sobre el control interno, entre otros aspectos relevantes.

## 5. MARCO DE REFERENCIA DE EVALUACIÓN DEL CONTROL INTERNO SOBRE REPORTE FINANCIERO

La documentación de los controles y el proceso de evaluación del Sistema de Control Interno sobre reporte financiero por parte de la Alta Dirección, bajo las reglas de la SEC, requieren que la Organización utilice un marco de control interno generalmente aceptado. Este marco de referencia define los elementos que se espera que estén presentes y funcionando en un Sistema de Control Interno efectivo. En la evaluación de efectividad, la Alta Dirección evalúa si el control interno sobre reporte financiero incluye políticas, procedimientos y actividades para cubrir los elementos que el marco de referencia establece.


Para dar cumplimiento a los requerimientos de la Ley SOX, La Organización se acoge al marco de referencia de control interno COSO 2013, el cual fue seleccionado por Grupo Aval, por considerar que es una buena práctica mundialmente reconocida. Este marco cuenta con tres objetivos de control (operaciones, reporte y cumplimiento), cinco componentes y 17 principios aplicables a toda la organización.



Los cinco componentes de control interno son:

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

Código: DG-0106/2

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 10 de 55
		Versión: 02
		Fecha: 01/06/2020

**Ambiente de control:** actividades y controles implementados por la Alta Dirección que establecen la forma de actuar de la organización y que se convierten en la base para los controles que se llevan a cabo en los procesos. Este componente se encuentra principalmente en Controles a Nivel de Entidad asociados al gobierno de la organización, niveles de delegación y responsabilidad, integridad y valores éticos.

**Evaluación de riesgos:** evaluación de los riesgos que pueden afectar el cumplimiento de los objetivos de la organización. Para el cumplimiento de la sección 404 de la Ley SOX, la administración debe identificar los riesgos asociados a error o fraude en los estados financieros, que pueden resultar de un error material en las cuentas significativas de los estados financieros.

**Actividades de control:** políticas, procedimientos y actividades que se llevan a cabo en toda la organización y en todos los niveles para aprobar, verificar, conciliar y revisar el cumplimiento de las operaciones y la adecuada segregación de funciones.

**Información y comunicación:** incluye los sistemas que soportan la captura e intercambio de información para llevar a cabo las actividades y la generación de la información financiera. Este componente incluye los ITGC sobre los sistemas de información a través de los cuales se acumula, procesa y autoriza las transacciones.

**Monitoreo:** proceso que la administración utiliza para evaluar la calidad del control interno. Incluye las actividades realizadas por los dueños de proceso como parte del monitoreo de las operaciones que se realizan, así como las evaluaciones que realiza la auditoría interna para evaluar la efectividad del control interno. Todas las actividades de monitoreo deben ser apropiadamente documentadas de tal forma que brinden evidencia de su ejecución.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

## 6. MODELO DE CUMPLIMIENTO SOX



### PLANEAR

- Acoger el alcance SOX definido y comunicado por Grupo Aval mediante instrucción corporativa, el cual es preparado con un enfoque basado en riesgos partiendo de lo general a lo particular “top down”, en el cual se definen cuentas contables, procesos y entidades o unidades de negocio sujetas a aseguramiento y que estén enmarcadas en la materialidad establecida por Grupo Aval, considerando los estados financieros consolidados del Grupo bajo normas IFRS y el riesgo general y relativo de error en las cuentas y revelaciones relacionadas con los estados financieros incluidos por casa matriz en el reporte 20F que envía a la SEC.
- Establecer las actividades a desarrollar para el cumplimiento de la metodología SOX con base en el calendario de fechas clave para el año objeto de aseguramiento, comunicado por Grupo Aval mediante instrucción corporativa.
- Acoger el inventario de riesgos SOX definidos por Grupo Aval para brindar aseguramiento a los procesos definidos bajo alcance.

### EVALUAR

- Evaluar la aplicabilidad de los riesgos definidos en el inventario de riesgos SOX para los procesos alcanzados en la Organización, justificando aquellos riesgos que no sean aplicables a la misma en el formato definido por Grupo Aval para tal fin.
- Identificar los controles que se tienen implementados en la organización para los riesgos existentes y documentarlos en la matriz SOX.
- Asegurar que los controles contenidos en las matrices SOX se encuentren debidamente documentados en manuales y/o procedimientos internos de la Organización. En algunas

situaciones especiales como reestructuraciones organizacionales, es posible que los documentos internos se encuentren en proceso de actualización; en estos casos se debe contar un plan de trabajo con fechas definidas y razonables considerando el tamaño de la reestructuración que se esté presentando.

- Asegurar que los controles se hayan comunicado a los colaboradores con el fin de que sean ejecutados conforme al diseño definido.
- Evaluar el diseño de los controles por parte de la Auditoría Interna para asegurar que cubran razonablemente los riesgos.

#### REMEDIAR

- Corregir las deficiencias de control identificadas por la Auditoría.

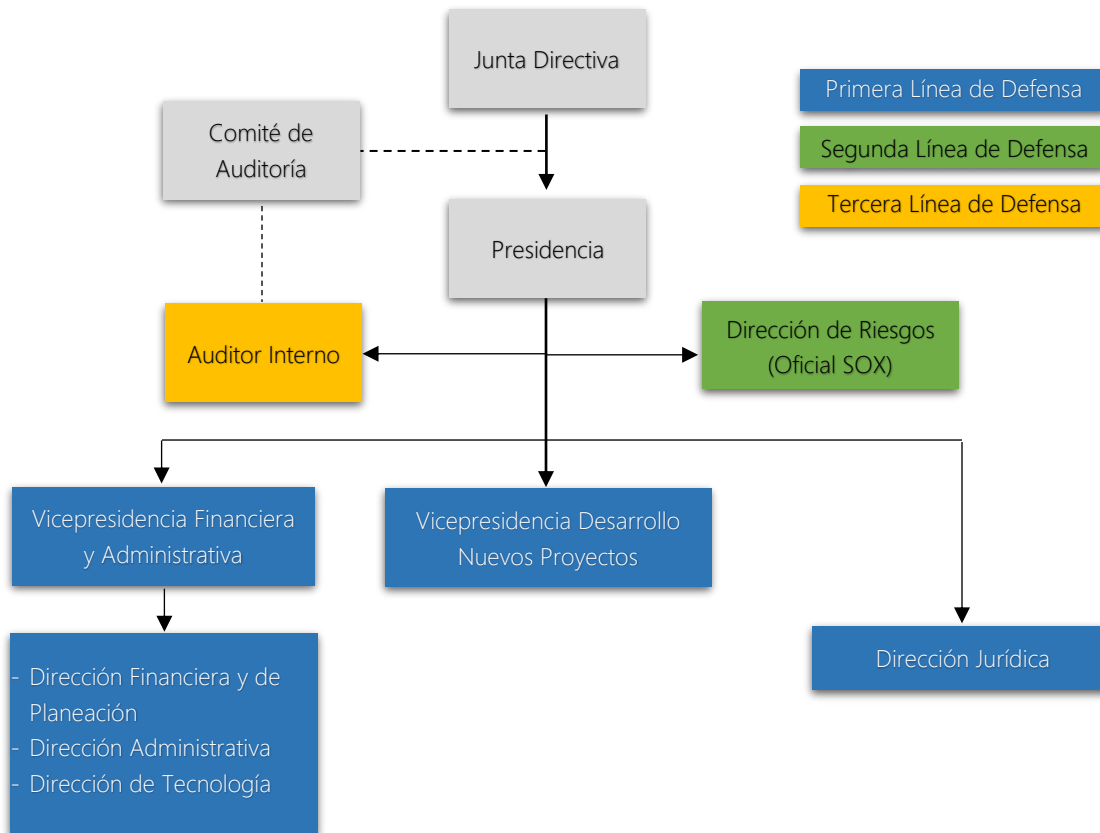
#### VALIDAR

- Evaluar la eficacia operativa de los controles a través de pruebas de auditoría, con el fin de validar que los controles funcionan tal y como se tienen diseñados y de forma uniforme a lo largo del periodo, para concluir si el Sistema de Control Interno sobre reporte financiero es efectivo.

#### REPORTAR

- Analizar y consolidar el efecto en el control interno de las deficiencias identificadas tanto en diseño como en efectividad de los controles.
- Cuantificar los impactos producidos por las deficiencias de control en el Reporte de Deficiencias de Control y los indicadores clave de riesgo en el Tablero de Control.
- Reportar a casa matriz el manifiesto o certificación de control interno sobre reporte financiero, según el alcance SOX definido a la Organización.


## 7. ORGANIGRAMA DE RESPONSABILIDAD FRENTE LA POLITICA



## 8. MODELO DE LAS TRES LINEAS DE DEFENSA

La Organización ha estructurado sus funciones y responsabilidades frente a sus riesgos, siguiendo la metodología de las tres líneas de defensa, considerando:

- La gestión propia del negocio.
- La función de riesgos de la organización.
- La función de auditoría interna.

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 14 de 55
		Versión: 02
		Fecha: 01/06/2020

### 8.1. PRIMERA LÍNEA DE DEFENSA

La primera línea de defensa la constituyen las áreas que gestionan el negocio y que son responsables de identificar, evaluar, gestionar y controlar los riesgos asociados a sus procesos. Esta línea debe conocer y aplicar las políticas, manuales y procedimientos definidos por la organización, así como disponer de los recursos suficientes para realizar eficazmente sus funciones.

### 8.2. SEGUNDA LÍNEA DE DEFENSA

La segunda línea de defensa la constituye el Oficial SOX y el equipo SOX, que hacen parte de la Dirección de Riesgos de la Organización. Son responsables de supervisar el cumplimiento de la metodología SOX definida por casa matriz, asistir a los dueños de proceso, así como de apoyar a la Presidencia y Vicepresidencia Financiera y Administrativa en el proceso de certificación de cumplimiento y evaluación y efectividad de control interno. El Oficial SOX deberá ser designado por la Presidencia y la Vicepresidencia Financiera y Administrativa de la Organización.

### 8.3. TERCERA LÍNEA DE DEFENSA

La tercera línea de defensa la constituye la función de Auditoría Interna de la Organización, la cual no participa en el desarrollo, implementación y operación de la estructura riesgo / control de esta. Se encarga de evaluar de forma independiente los riesgos y controles SOX diseñados por los dueños de proceso de acuerdo con su plan de trabajo.

## 9. ROLES Y RESPONSABILIDADES PARA EL CUMPLIMIENTO SOX

Los roles y responsabilidades establecidas en la organización para asegurar el cumplimiento SOX son los siguientes:

### 9.1. JUNTA DIRECTIVA

- Asegurar que la Alta Dirección tenga implementado un adecuado Sistema de Control Interno sobre reporte financiero.
- Estar informado sobre el alcance SOX definido por Grupo Aval para la Organización, así como de los resultados del proceso SOX.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

- Recibir información relevante de cualquier incidente de fraude o cualquier falla importante en el control interno que afecte los estados financieros.
- Estar enterado de las conclusiones de la evaluación de control interno sobre reporte financiero de la Organización.
- Realizar seguimiento semestral al informe presentado por el Vicepresidente Financiero y Administrativo o Representante Legal sobre los resultados obtenidos frente a la identificación, medición y control de los riesgos.

## 9.2. COMITÉ DE AUDITORIA

- Evaluar el informe presentado por el Auditor Interno, sobre la gestión y evaluación de la eficacia del Sistema de Control Interno, incluyendo todos sus elementos, por lo menos, al cierre de cada ejercicio.
- Velar porque la preparación, presentación y revelación de la información financiera se ajuste a lo dispuesto en las normas aplicables, verificando que existen los controles necesarios.
- Estudiar los estados financieros y elaborar el informe correspondiente para someterlo a consideración de la Junta Directiva, con base en la evaluación no sólo de los proyectos correspondientes, con sus notas, sino también de los dictámenes, observaciones de los órganos de control, resultados de las evaluaciones efectuadas por los comités competentes y demás documentos relacionados con los mismos.

## 9.3. PRESIDENCIA Y VICEPRESIDENCIA FINANCIERA Y ADMINISTRATIVA

- Velar por el establecimiento de un apropiado Sistema de Control Interno sobre reporte financiero.
- Asegurar la efectividad del Sistema de Control Interno sobre los procesos y controles que están a su cargo.
- Informar al presidente y Vicepresidente Financiero de casa matriz sobre los resultados del control interno, en especial si existen aspectos que puedan afectar el control interno de la Organización.
- Revisar los reportes de auditoria (interna y externa) para identificar el efecto en sus procesos y controles, así como tomar los correctivos correspondientes.
- Efectuar seguimiento al Reporte de Deficiencias de Control (RDC) generado el año inmediatamente anterior y asegurar que se implementen los correctivos oportunamente.

- Alertar al Oficial SOX y al área de riesgos sobre cambios en la operación, riesgos y/o responsables.
- Designar al Oficial SOX de la Organización y proveer los recursos necesarios para la ejecución de su labor.
- Velar por la adecuada y oportuna aplicación de los planes de remediación que sean necesarios para minimizar el riesgo de error en los estados financieros.
- Obtener los manifiestos o certificaciones SOX de las sociedades de Infraestructura bajo alcance SOX para soportar a su vez, el manifiesto o certificación de control interno sobre reporte financiero de Proindesa S.A.S.
- Firmar el manifiesto o certificación de control interno sobre reporte financiero, asegurar que cuente con los soportes respectivos y emitirla al Presidente y Vicepresidente Financiero de casa matriz o quien haga sus veces.
- Certificar la evaluación de riesgo a nivel de entidad para la determinación del alcance anual.

#### 9.4. DUEÑOS DE PROCESO O CONTROLES

- Diseñar e implementar los controles necesarios para mitigar los riesgos asociados con sus responsabilidades, con el acompañamiento del Oficial SOX de Proindesa S.A.S., asegurando su implementación y ejecución permanente.
- Actuar como dueños primarios de su respectivo proceso o control para asegurar la adecuada documentación de estos.
- Conocer y entender los riesgos y controles a su cargo y su importancia dentro del proceso alcanzado.
- Asegurar la correcta documentación de las evidencias que soportan los controles a cargo.
- Suministrar la información relacionada con evidencia de los controles a su cargo, a los órganos de control de forma completa y oportuna.
- Informar al Oficial SOX y al Vicepresidente o Gerente o Director del Área, sus necesidades de capacitación relacionadas con el control interno y el proceso SOX.
- Informar al Oficial SOX y al Vicepresidente o Gerente o Director del Área, los cambios realizados a las actividades de control, procesos o sistemas de información para que sea actualizada la matriz SOX de riesgos y controles clave.
- Realizar monitoreo de controles para asegurar que estos mitigan los riesgos y se encuentren vigentes, documentados, comunicados y ejecutados apropiadamente de manera uniforme durante todo el período.



- Diseñar los planes de remediación con el apoyo del Oficial SOX y ponerlos en marcha de forma inmediata.
- Estar informados de los resultados de las pruebas de diseño y eficacia operativa de los controles y participar en el proceso de discusión de estos.
- Informar oportunamente al Oficial SOX cuando identifique alguna falla en la efectividad del control, producto de la ejecución de este.
- Velar por la continua aplicación de los controles y su respectiva documentación a lo largo del periodo.
- Actualizar la matriz con el apoyo del Oficial SOX cada vez que se presenten cambios en riesgos y/o controles.
- Realizar el empalme adecuado, suficiente y oportuno en caso de retiro temporal o permanente.
- Velar por que los hallazgos de diseño y efectividad operativa reportados por la auditoría interna y/o externa, sean remediados en el transcurso del año. Para aquellos hallazgos que sean identificados al cierre del ejercicio, deben velar por que se cuente con controles compensatorios suficientes y en todo caso, asegurar que los planes de acción se implementen oportunamente.

#### 9.5. OFICIAL SOX

- Apoyar al Vicepresidente Financiero y Administrativo en la documentación de asuntos clave a considerar en la planeación SOX.
- Asistir al Oficial SOX Corporativo en la identificación de aspectos cualitativos y/o cuantitativos que se deben considerar en el proceso de definición del alcance.
- Apoyar a los dueños de proceso y controles en la calificación de riesgo del control.
- Asesorar a los dueños de proceso y controles en la identificación de la totalidad de los controles que se requieren para mitigar razonablemente los riesgos clave SOX.
- Asegurar que las comunicaciones y directrices emitidas por casa matriz fueron entendidas y aplicadas en la Organización., a través del Oficial SOX.
- Actuar como primer contacto al interior de la organización, para la coordinación de las tareas a realizar en cumplimiento de la evaluación del control interno bajo normativa SOX.
- Efectuar seguimiento a las acciones realizadas por los dueños de proceso o controles en el aseguramiento de diseño de controles en la Organización.
- Identificar y tramitar las necesidades de entrenamiento SOX al interior de la Organización y

comunicarlas al Oficial SOX Corporativo, así como compartir el conocimiento SOX al interior de la organización.

- Monitorear el desarrollo del proceso SOX en la Organización.
- Acompañar a los dueños de proceso o controles en el cumplimiento de la metodología SOX, el aseguramiento del diseño y operatividad de los controles y en el diseño de planes de remediación.
- Asegurar que los dueños de proceso actualicen anualmente la documentación de los controles en la matriz y dejar evidencia de dicha actualización mediante actas.
- Reportar al Oficial SOX de casa matriz el avance del trabajo, las deficiencias identificadas y otros temas que puedan ser considerados como clave para la evaluación de SOX.
- Participar en el proceso de cuantificación de las deficiencias que no fueron remediadas y en la identificación de controles compensatorios.
- Consolidar los informes de Proindesa S.A.S y las sociedades de Infraestructura bajo alcance SOX requeridos y reportarlos al Oficial SOX de casa matriz.
- Apoyar al Presidente y Vicepresidente Financiero y Administrativo de Proindesa S.A.S. en la emisión de la certificación o manifiesto de control interno sobre reporte financiero.
- Mantener la información del proceso SOX de la Organización de forma completa, precisa y segura, así como desarrollar y establecer los mecanismos que le permitan asegurar que la documentación de las pruebas de validación de los controles está siendo debidamente custodiada en la Organización.
- Custodiar las matrices, asegurar el apropiado control de versiones y mantener actualizado el control de cambios de cada una, con el fin de exponer las inclusiones, modificaciones o eliminaciones de riesgos y/o controles en la organización.
- Hacer seguimiento a las deficiencias no remediadas en periodos anteriores.
- Asegurar la integridad y exactitud del Reporte de Deficiencias de Control (RDC), incluyendo la cuantificación de impacto y probabilidad de ocurrencia.
- Preparar el Tablero de Control de la Organización y consolidar los de las sociedades de Infraestructura bajo alcance SOX para el reporte a casa matriz.

## 9.6. AUDITORIA INTERNA

- Adquirir el entendimiento de los procesos y controles a ser validados a través de normas y buenas prácticas de auditoría aplicables al control interno sobre la información financiera.
- Realizar y documentar la evaluación independiente del diseño de los controles, de acuerdo

con su plan de trabajo aprobado por el Comité de Auditoría.

- Realizar la validación independiente de la efectividad de los controles de acuerdo con el plan de trabajo aprobado por el Comité de Auditoría.
- Informar al presidente, Oficial SOX, Vicepresidente Financiero y Administrativo y dueños de proceso o controles sobre los resultados de la evaluación de diseño y eficacia operativa de los controles.
- Emitir reportes periódicos que incluyan el avance y los resultados obtenidos de las pruebas de diseño y operatividad dirigidos al Oficial SOX de la organización.

#### 9.7. GESTIÓN DE CALIDAD (O QUIEN HAGA SUS VECES)

- Apoyar en el aseguramiento de diseño de controles a través de la apropiada documentación de las actividades de control en los manuales y/o procedimientos de la organización.
- Publicar y divulgar a los interesados las Políticas, Manuales y/o Procedimientos de sus áreas o procesos cargo.
- Asegurar que todo cambio realizado en los procesos sea actualizado en el documento respectivo.

#### 9.8. TODOS LOS COLABORADORES

- Ejecutar adecuadamente sus procesos.
- Evaluar y controlar su trabajo.
- Detectar desviaciones y emitir las alertas que consideren necesarias con el fin de propender por el cumplimiento de las actividades establecidas.
- Asegurar un adecuado Sistema de Control Interno.

### 10. ENFOQUE SOX

#### 10.1. ENFOQUE 1 (ENFOQUE COMPLETO)

Este enfoque comprende los siguientes aspectos:

- Preparación de matrices SOX de riesgo control clave para los procesos bajo alcance SOX definidos por Grupo Aval mediante instrucción corporativa.

- Aseguramiento del diseño y de la operatividad para todos los controles por parte de los dueños de proceso, con el acompañamiento de los equipos SOX.
- Mantenimiento de matrices actualizadas y alineadas con el diseño por parte de los dueños de proceso con el acompañamiento y control de cambios de los equipos SOX.
- Desarrollo del plan de trabajo por parte de los Auditores Internos.
- Reporte de avance y resultados a los equipos SOX de Proindesa S.A.S. y de casa matriz.
- Certificación del Presidente y Vicepresidente Financiero.

## 10.2. ENFOQUE 2 (ENFOQUE PARTICULAR)

Este enfoque comprende los siguientes aspectos:

- Preparación de matrices SOX de riesgo control clave para los procesos significativos identificados en la organización.
- La matriz SOX debe incluir riesgos asociados con segregación de funciones, asignación de accesos, derivados implícitos, contratos anexos, contratos de arrendamiento, independiente del proceso que tenga alcanzado. Estos riesgos deben asociarse al proceso alcanzado.
- Incluir los controles asociados a los procesos de migración y adquisición de negocios, cuando sucedan estos eventos.
- Incluir en la matriz SOX los controles de revisión de la gerencia (MRC) relacionados con razonabilidad de los estados financieros.
- Aseguramiento del diseño y de la operatividad para todos los controles por parte de los dueños de proceso, con el acompañamiento del equipo SOX.
- Mantenimiento de matrices actualizadas y alineadas con el diseño por parte de los dueños de proceso con el acompañamiento y control de cambios de los equipos SOX.
- Desarrollo del plan de trabajo por parte de los Auditores Internos.
- Reporte de avance y resultados a los equipos SOX de Proindesa S.A.S. y de casa matriz.
- Manifiesto del Presidente y Vicepresidente Financiero (o quien haga sus veces) con respecto al control interno sobre financiero.

## 10.3. OTRAS ENTIDADES

Para las entidades con riesgo bajo, se requiere que los encargados de la preparación y revisión de los estados financieros (Gerente General y Director Financiero y de Planeación, o quien haga sus veces) presenten una comunicación en donde se informe si sus auditores internos, externos o revisores fiscales

han reportado asuntos importantes que indiquen deficiencias sobre el funcionamiento de los aspectos relevantes al control interno sobre reporte financiero. Normalmente esta comunicación se sustenta con el informe de Gestión de la Alta Dirección y/o la opinión del Revisor Fiscal sobre los estados financieros.

## 11. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS


### 11.1. RIESGO SOBRE REPORTE FINANCIERO EXTERNO

El principal objetivo del control interno sobre reporte financiero es emitir información financiera confiable, esto es, libre de errores materiales generados por error o fraude. Por lo cual, la Alta Dirección debe suministrar estados financieros que presenten fielmente la posición financiera de la compañía, los resultados de las operaciones y los flujos de efectivo de acuerdo con los principios contables aplicables.

Las debilidades en la presentación razonable surgen cuando uno o más importes o revelaciones de los estados financieros contienen declaraciones equivocadas, incluyendo omisiones que sean materiales. Por lo cual, se deben identificar y valorar aquellos riesgos que, individualmente o en combinación con otros, pudieran resultar en una declaración equivocada material del reporte financiero.

El riesgo sobre reporte financiero incluye eventos externos e internos, transacciones o circunstancias que podrían afectar de manera adversa la capacidad de la Organización para iniciar, registrar, procesar y reportar datos financieros de manera consistente con las aserciones de la Alta Dirección en los estados financieros. Incluye los **riesgos de error material** en las cuentas significativas, revelaciones y aserciones asociadas y el **riesgo de fraude** que se entiende como el riesgo de error material sobre los estados financieros debido a la acción intencional cometida por un colaborador para asegurar una ganancia injusta o indebida, que conlleva a que una aserción relevante asociada con saldos, clases de transacciones o revelaciones, contenga errores que pudieran ser materiales, de manera individual o agregada con otros errores, en los estados financieros.

De acuerdo con la metodología establecida por Grupo Aval, los riesgos sobre reporte financiero (SOX) aplicables para el año objeto de aseguramiento, son establecidos en el Inventario de Riesgos Genéricos, el cual es comunicado mediante Instrucción a todas las filiales del Grupo para su aplicación y evaluación en cada uno de los procesos alcanzados. El Inventario de Riesgos Genéricos se presenta a nivel de proceso, relaciona los riesgos vigentes, aserciones y transacciones, indica si el riesgo está asociado a riesgo de fraude, evaluación de la calificación de la magnitud del impacto, probabilidad de ocurrencia

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 22 de 55
		Versión: 02
		Fecha: 01/06/2020

y determinación de la calificación del riesgo inherente. Este documento no está sujeto a ningún tipo de modificación por parte de la Organización.

## 11.2. EVALUACIÓN DEL RIESGO INHERENTE

El riesgo inherente es la susceptibilidad de que los estados financieros presenten un error, asumiendo que no existen controles para mitigarlo, o la susceptibilidad de que una aserción relevante de los estados financieros a que se incurra en un error (por error o fraude), pudiera ser material en los estados financieros de manera individual o agregada con otros errores, asumiendo que no hay controles internos.

## 11.3. ESCALAS DE CALIFICACIÓN

La Organización se acoge a la metodología de calificación del riesgo inherente para cada uno de los riesgos SOX, los cuales son valorados por el equipo SOX de Grupo Aval en cuanto a Magnitud de Impacto y Probabilidad de Ocurrencia, cuyos factores, explicaciones, calificaciones y ponderaciones están definidos en el Manual Corporativo de Cumplimiento Ley SOX.

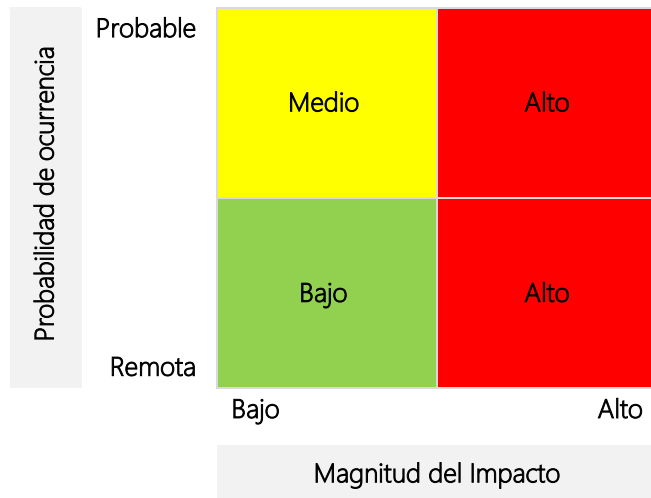
Los riesgos SOX se actualizan con una periodicidad anual, durante el primer trimestre del año y cada vez que lo requiera Grupo Aval, considerando la instrucción corporativa de actualización, modificación o inclusión de riesgos nuevos en el "Inventario de Riesgos Genéricos" vigente para el año objeto de aseguramiento. La información asociada al inventario de riesgos genéricos, así como las calificaciones de los riesgos inherentes solo puede ser modificada por el equipo SOX de Grupo Aval.

El nivel de riesgo inherente establecido en el "Inventario de riesgos genéricos" debe ser utilizado por el Oficial SOX y los dueños de proceso para valorar de forma independiente el Nivel de Atención Requerido del Control (NAR) asociado a cada control.

Los riesgos SOX son clasificados en categorías alto o bajo de acuerdo con la Magnitud de Impacto y la Probabilidad de Ocurrencia. El resultado de la ponderación de la magnitud del impacto y de la probabilidad de ocurrencia, estimando que los dos factores tienen el mismo peso, considera el mapa de riesgo que se visualiza a continuación:

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

MAPA DE RIESGO INHERENTE



11.4. RIESGO DE FALLA DEL CONTROL

Debido a las limitaciones inherentes al control interno, existe la posibilidad de que alguno de los controles falle y ocurra un error material en el reporte financiero, que no sea oportunamente prevenido o detectado.

Por lo anterior, el dueño de proceso con el apoyo del Oficial SOX debe calificar los factores que determinan el riesgo de falla del control, que corresponden a:

- Actividades complejas en la operación del control.
- Juicios significativos en la operación del control.
- Efectividad del control que depende de la efectividad de otros controles SOX.
- Ejecución en múltiples localidades.
- Controles que abarcan más de dos aserciones.
- Cambios en el volumen o naturaleza de las transacciones que puedan afectar adversamente el diseño o la efectividad de los controles.
- Errores o ajustes significativos en la cuenta asociada.
- Controles manuales.
- Cambios en el personal clave que desarrolla el control o monitorea su ejecución.
- Cambios en las aplicaciones o ADUs que respaldan el control.

### 11.5. CRITERIOS DE EVALUACIÓN

Con base en la metodología establecida por Grupo Aval, se deben considerar las siguientes ponderaciones asociadas a cada factor, las cuales dependen de su efecto en el incremento de la posibilidad de que el control falle:


No.	Factores	Ponderación	
		Si	No
1	¿La operación del control tiene actividades complejas?	10%	0%
2	¿La operación del control requiere de juicios significativos en la operación del mismo?	10%	0%
3	¿La efectividad del control depende de la efectividad de otros controles SOX?	5%	0%
4	¿El control se ejecuta en múltiples localidades?	10%	0%
5	¿El control opera para más de dos aserciones?	5%	5%
6	¿Han existido cambios en el volumen o naturaleza de las transacciones que puedan afectar adversamente el diseño o la efectividad de los controles?	10%	0%
7	¿Han existido errores o ajustes significativos en la cuenta asociada?	10%	5%
8	¿El control es manual?	10%	5%
9	¿Han existido cambios en el personal clave que desarrolla el control o monitorea su ejecución?	5%	0%
10	¿Han existido cambios importantes en las aplicaciones o ADU que respaldan el control?	5%	0%

### 11.6. CALIFICACIÓN DEL NIVEL DE ATENCIÓN REQUERIDO (NAR)

El Nivel de Atención Requerido, está conformado por el nivel de riesgo inherente y los diez factores asociados al riesgo de falla de control. La calificación del riesgo inherente establecida en la matriz SOX, debe ser consistente con la definida en el "Inventario de riesgos genéricos" vigente.

Conforme a la metodología establecida en el Manual Corporativo de Cumplimiento Ley SOX, un riesgo inherente alto tendrá un peso de 20% dentro de la determinación final del Nivel de Atención Requerido



 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 25 de 55
		Versión: 02
		Fecha: 01/06/2020

de cada control. En cambio, un riesgo inherente bajo tendrá un peso de 5% dentro de la determinación final del NAR asociado a dicho control.

No.	Factor a ser considerado en el NAR	Ponderación	
		Si	No
1	¿El riesgo inherente asociado con las cuentas y aserciones relacionadas es alto?	20%	5%

Asimismo, se deberán evaluar los factores mencionados en el numeral 11.5, respondiendo “Si” o “No” según corresponda para cada uno de los controles. Una vez se adicionen las calificaciones de los factores asociados con el riesgo de falla del control, se debe generar la sumatoria de los porcentajes para determinar la calificación del Nivel de Atención Requerido, considerando las siguientes ponderaciones:

Nivel de Atención Requerido (NAR)	Ponderación	Descripción
Alto	Mayor a 40%	La probabilidad de que el control falle es alta y se encuentra asociado a un riesgo inherente calificado como alto, por lo tanto, es necesario que la Alta Dirección profundice sobre las causas de las fallas en el control y establezca con carácter prioritario planes de remediación que conlleven a que el riesgo de falla de control disminuya.
Bajo	Menor o igual a 40%	La efectividad del control mitiga el riesgo inherente en un porcentaje significativo, pues no se esperan fallas en el mismo. Es probable que no se requiera implementar controles adicionales ni planes de acción.

La Organización debe mitigar los riesgos de tal forma que su impacto residual, individual o agregado en caso de falla de control no sea superior a la materialidad para las cuentas significativas definida por Grupo Aval. En caso de que el riesgo se materialice, el costo de los controles no debe exceder el valor del impacto generado por el riesgo.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

### 11.7. Calificación del Nivel de Atención Requerido (NAR) para aplicaciones relevantes

Las aplicaciones relevantes que utiliza la organización deben listarse y evaluarse haciendo uso del formato "Inventario de aplicaciones SOX" establecido por Grupo Aval. Asimismo, las aplicaciones incluidas en el inventario deben tener por lo menos un control asociado dentro de la Matriz SOX.

Lo anterior, con el fin de obtener una evaluación del nivel de relevancia de las aplicaciones, determinar si está debe estar incluida en el alcance de aplicaciones SOX y en caso de resultar alcanzada, identificar cual es el nivel mínimo de aseguramiento.

El puntaje para la clasificación del nivel de relevancia de las aplicaciones es el siguiente:

Nivel de Relevancia SOX	Puntaje
Bajo	Menor o igual a 15 Mayor que 15 y menor o igual a 40
Alto	Mayor que 40

La clasificación del nivel de relevancia para aplicaciones SOX, toma en cuenta el nivel de importancia que tiene la aplicación para los estados financieros, como la probabilidad de falla de esta, los dos criterios se miden en el formato Inventario de Aplicaciones SOX a través de los siguientes factores de riesgo:

- Importancia de la aplicación para los estados financieros: inicio, autorización, procesamiento y contabilización de transacciones.
- Historial de errores, fallas de la aplicación, cambios de emergencia o nivel de personalización.
- Naturaleza de la tecnología: lógica de procesamiento distribuida en varias capas, intervención manual de TI, nuevas versiones o módulos, lógica de procesamiento, interfaces, entre otros.
- Suficiencia del personal que soporta el ambiente de procesamiento.

El Oficial SOX de la Organización en conjunto con los dueños de proceso, debe evaluar el nivel de relevancia generado por el Inventario de aplicaciones y ratificar la calificación a través de la asignación del nivel de atención requerido de la aplicación, para esto se tienen en cuenta los siguientes aspectos:

1. **Aplicaciones con nivel de relevancia "3"**: aplicaciones con un impacto directo sobre el proceso de información financiera o con un alto grado de falla. Su nivel de atención requerido es "Alto".
2. **Aplicaciones con nivel de relevancia "2"**: aplicaciones con un nivel medio de afectación sobre los estados financieros y una probabilidad de falla media. Su nivel de atención requerido es "Bajo".
3. **Aplicaciones con nivel de relevancia "1"**: para las aplicaciones que clasifiquen en esta categoría, el equipo SOX en conjunto con el dueño del proceso y el administrador técnico de la aplicación, deben analizar si el (los) control (es) soportados por la aplicación son controles clave para el cubrimiento de los riesgos asociados o si pueden existir otros controles en aplicaciones con nivel de relevancia "2" o "3" que puedan estar mitigando el mismo riesgo. En cuyo caso se deben realizar los correspondientes ajustes sobre los controles.


## 12. ACTIVIDADES DE CONTROL

Los controles son actividades realizadas sobre el inicio, registro, procesamiento, monitoreo y reporte de las transacciones, que están diseñados específicamente para prevenir o detectar y corregir oportunamente errores en los estados financieros y para mitigar los riesgos inherentes identificados en los procesos.

Las actividades de control ofrecen a la Alta Dirección una garantía razonable para el cumplimiento de los objetivos y minimizan la posibilidad de que se materialice el riesgo. Los principales objetivos de los controles son:

- Salvaguardar activos.
- Verificar la adecuación, fiabilidad, consistencia e integridad de la información.
- Promover la eficacia operacional.
- Fomentar la adherencia al cumplimiento de las políticas establecidas y/o regulación aplicable.

Los dueños de proceso deben identificar los controles necesarios para mitigar los riesgos SOX de su proceso, con el apoyo del Oficial SOX de la organización, considerando las líneas base emitidas por Grupo Aval y los lineamientos establecidos para asegurar el diseño de estos.

	<p style="text-align: center;">POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</p>	Página 28 de 55
		Versión: 02
		Fecha: 01/06/2020

Los controles pueden tener las siguientes características:

Según su naturaleza,

- **Controles automáticos:** Realizados por sistemas computarizados de manera regular y sistémica, en respuesta a condiciones predeterminadas (parametrización), no requieren la intervención manual.
- **Controles manuales:** Ejecutados por un colaborador de la Organización, sin apoyo tecnológico o con apoyo parcial.

Según su tipo,

- **Preventivos:** Son aquellos que tienen el propósito de prevenir errores o fraude, que podrían resultar en errores en los estados financieros.
- **Detectivos:** Son aquellos cuyo propósito es detectar errores, debido a error o fraude, en los estados financieros.

Según su nivel en la compañía,

- **Controles a nivel de entidad:** conocidos como ELC (Entity Level Controls), operan a nivel de toda la entidad y a menudo tienen un impacto generalizado sobre los controles a nivel de procesos, transacciones o aplicativos. La efectividad de los ELC para detectar o prevenir errores en los estados financieros, varía según su naturaleza y nivel de precisión.
- **Controles Generales de Información Tecnológica (ITGC):** incluyen políticas y procedimientos relacionados con las aplicaciones y respaldan el funcionamiento efectivo de la aplicación de controles al ayudar a garantizar la operación continua apropiada de los sistemas de información. Esto abarca cuatro áreas básicas que son relevantes para el control interno de reporte financiero: desarrollo de programas, operaciones de computador, mantenimiento a programas y accesos a los programas y datos.
- **Controles a nivel de proceso o transacción:** actividades de control sobre inicio, registro,

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

procesamiento y reporte de transacciones diseñadas para operar, a un nivel de precisión tal, que podrían prevenir o detectar y corregir oportunamente errores en una o más manifestaciones relevantes de una cuenta de los estados financieros.

Los controles pueden corresponder a:

- **Autorización:** aprobación de transacciones ejecutadas de acuerdo con las políticas de la organización. Aseguran que solamente cargos autorizados puedan iniciar, modificar, anular o borrar transacciones o que ciertos cargos no puedan iniciar transacciones.
- **Reconciliación:** diseñados para verificar si la información financiera o los registros de dos fuentes son consistentes a través de la comparación contra fuentes independientes.
- **Controles de Revisión de la Gerencia: conocidos como MRC (Management Review Controls):** involucran a los miembros de la Alta Dirección con el fin de analizar, revisar y/o evaluar sobre ciertas actividades y controles desarrollados por otros colaboradores (típicamente un subordinado) y concluir sobre la información financiera, gestión y/o resultados. La documentación de la evidencia de estos controles debe seguir los parámetros establecidos en el Manual Corporativo de Cumplimiento Ley SOX de Grupo Aval.
- **Revisiones de desempeño:** son evaluaciones cuantitativas financieras y/o no financieras que son realizadas por la organización y utilizadas por la Alta Dirección para evaluar el grado de avance respecto a una meta de desempeño. Incluye las revisiones analíticas de información actual respecto a planes o presupuestos. Cuando este tipo de revisiones incluyen como objetivo la identificación de errores en el reporte financiero, y el nivel de precisión de estos controles es suficiente para lograr dicho objetivo, el control podría ser clave para SOX
- **Segregación de funciones:** es la separación de tareas y responsabilidades de autorización, contabilización, procesamiento y control de transacciones para prevenir que algún individuo esté en posición de incurrir en un error o irregularidad. Incluye el hecho de prevenir que un mismo colaborador pueda iniciar y autorizar una transacción.
- **Excepción / reportes de edición:** se refiere a cuando un reporte es generado comúnmente por un sistema de manera automática o por la interacción humana, para monitorear ciertas


excepciones o transacciones con la misma intención de hacer seguimiento a ítems inusuales a través de la investigación y solución de estos.

- **Configuración / Controles de asignación de cuentas / Edición y Validación (procesamiento de información):** permiten validar los atributos de los datos que ingresan al sistema, incluye aplicaciones estándar o ajustadas, diseñadas con base en criterios de negocio apropiados.
- **Controles de configuración:** definición lógica en los sistemas para restringir el procesamiento de datos inapropiados.
- **Asignación de cuentas:** definición lógica en los sistemas de cómo una transacción es registrada en los estados financieros.
- **Interfaz:** la transferencia de datos a través de interfaces implica que la información se mueve entre dos sistemas o aplicaciones. Los controles relacionados aseguran la integridad y exactitud de los datos transferidos.
- **Acceso a los sistemas:** controles relacionados con el acceso a solo algunos colaboradores a las diferentes opciones en los sistemas de información.
- **Controles de aplicación:** procedimientos manuales o automatizados que típicamente operan a nivel de los procesos de negocio y aplican para el procesamiento de las transacciones en los sistemas individuales. Estos pueden ser preventivos o detectivos y son diseñados para asegurar la integridad de los registros contables.

También se refieren a los procedimientos utilizados para iniciar, registrar, procesar y reportar las transacciones u otros datos financieros. Estos controles ayudan a asegurar que las transacciones ocurrieron, son autorizadas y son registradas y procesadas de manera correcta y exacta.

## 12.1. ENFOQUE PARA LA IDENTIFICACIÓN DE CONTROLES CLAVE

La Alta Dirección debe evaluar si tiene controles en operación que estén diseñados para administrar adecuadamente los riesgos sobre reporte financiero. Los controles que la Alta Dirección identifica y documenta son aquellos que son importantes (clave) para cumplir los objetivos de control interno

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 31 de 55
		Versión: 02
		Fecha: 01/06/2020

sobre reporte financiero.

Los controles identificados como clave para cada Riesgo SOX se detallan por proceso alcanzado en la herramienta denominada "Matriz SOX", la cual facilita la identificación de los controles que se consideran clave para el control interno sobre reporte financiero. En ningún caso, la matriz reemplaza los manuales o procedimientos internos que documentan los procesos de la Organización.


Antes de finalizar el primer semestre del año, los dueños de proceso con el apoyo del Oficial SOX deben identificar controles clave (ya sean controles nuevos o existentes), revisar y asegurar el diseño de estos considerando el inventario de riesgos genéricos, las oportunidades de mejora y hallazgos identificados por la auditoría interna, planes de acción y recomendaciones emitidas por el Oficial SOX.

La identificación de controles clave inicia con el proceso de análisis de riesgos sobre reporte financiero, identificando controles de más alto nivel, es decir, controles de revisión de la gerencia (MRC) y bajando hasta nivel transaccional en donde sea necesario, considerando los siguientes aspectos:

- Nivel de competencia, grado de responsabilidad, autoridad y decisión de quien ejecuta el control. Entre mayor sea el nivel del dueño de proceso, mayor poder de toma de decisión tendrá sobre los resultados del control.
- La selección de controles debe ser una mezcla de varios tipos de control. Comúnmente, un solo tipo de control no es suficiente para cubrir los riesgos a lo largo de todo el proceso.
- Se deben considerar controles manuales y automáticos, dando prioridad a estos últimos dado que el riesgo que fallen es menor.
- Deben considerarse controles que aseguren una apropiada segregación de funciones (registro, revisión, autorización, seguimiento, entre otros), así como aquellos controles alternos cuando no se pueda segregar apropiadamente las funciones.
- Deben estar diseñados con frecuencia y oportunidad apropiadas para la mitigación del riesgo.
- Entre más aserciones cubra un mismo control, mayor será su importancia para brindar aseguramiento SOX.

La cantidad de controles a identificar y/o implementar para cada riesgo dependerá del grado de aversión al mismo, siempre y cuando, la agregación de impactos en caso de falla de los controles no sea superior a la materialidad para las cuentas significativas definidas por Grupo Aval y el conjunto de controles mitigue el riesgo para todas las aserciones clave asociadas al riesgo.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 32 de 55
		Versión: 02
		Fecha: 01/06/2020

## 12.2. DISEÑO ADECUADO DE CONTROLES


El diseño de los controles debe considerar los siguientes aspectos:

- a. Los controles SOX, deben estar documentados y oficializados en un manual o procedimiento
- b. y debidamente comunicados a los responsables.
- c. El control debe ser coherente en relación con el riesgo asociado, por tanto, debe mitigarlo.
- d. La persona que ejecuta el control debe tener el conocimiento y la experiencia requeridos.
- e. En ningún caso un control SOX podrá ser ejecutado por personal con vinculación temporal a la organización.
- f. Debe existir segregación de funciones entre el inicio, autorización, procesamiento, contabilización, reporte y control de transacciones.
- g. La información utilizada para realizar el control debe ser confiable e íntegra.
- h. Las excepciones identificadas al realizar el control deben ser investigadas y resueltas oportunamente.
- i. La redacción de los controles debe ser comprensible para cualquier lector, exponiendo claramente la acción que realizan y debe indicar: título del control, quien lo ejecuta con su respectivo backup, cuál es la actividad de control, frecuencia, como se realiza, qué evidencia se deja y donde se custodia la información. En ningún caso, un control deberá ser una extensión de los procedimientos internos que respaldan cada proceso.
- j. La evidencia de los controles debe estar documentada por parte de los dueños de proceso con suficiente nivel de detalle, en mecanismos adecuados de custodia y archivo con el fin de que esté disponible para los órganos de control.
- k. Se debe determinar la tipología de los controles: preventivo, para aquellos cuyo propósito es evitar una materialización del riesgo; y detectivo, para aquellos cuyo objetivo es detectar desviaciones frente a lo establecido.
- l. Se debe establecer la naturaleza del control: manual o automático.
- m. Las actividades de control pueden ser reprocesadas (para efectos de una revisión independiente), en cuanto a la generación de reportes y listados sobre los cuales se ejecuta el control.
- n. Todos los controles deben contar con la calificación del Nivel de Atención Requerido (NAR) en la Matriz SOX, la cual se actualiza por lo menos anualmente o cada vez que se presenten cambios reportados mediante instrucción corporativa por parte de Grupo Aval.
- o. Los controles de resultados que se incluyan en las matrices SOX deben ejecutarse sobre los saldos acumulados a la fecha de la primera evidencia y en lo sucesivo, podrá cubrir solo el

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**



 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 33 de 55
		Versión: 02
		Fecha: 01/06/2020

movimiento que corresponda a la frecuencia del control.

### 12.3. CONTROLES A NIVEL DE ENTIDAD (ELC)

Son controles que operan a nivel de toda la organización y tienen un impacto generalizado sobre los controles a nivel de procesos, transacciones o aplicativos. La efectividad de los controles a Nivel de Entidad para detectar o prevenir errores en los estados financieros, varía según su naturaleza y su nivel de precisión:


- Controles indirectos y generalizados: no están relacionados con una cuenta específica, proceso o aserción, pero pueden contribuir a la efectividad de otros controles. Este tipo de controles que están relacionados con el ambiente de control son importantes, porque éste representa el fundamento a partir del cual se basan todos los componentes del control interno y por tanto establece el tono de la organización.
- Controles que monitorean otros controles: realizan vigilancia de las operaciones y la efectividad de los otros controles. Abordan el riesgo de que la Alta Dirección eluda los controles e influyen en mantener una cultura corporativa donde la integridad y los valores éticos sean tenidos en cuenta.
- Controles directos y precisos: operan a nivel de subproceso, pueden prevenir o detectar un error material si se ejecuta con un nivel de precisión suficiente.

Los siguientes son ejemplos de controles a nivel de entidad:

- Filosofía de la administración y estilo de operación
- Integridad y valores éticos
- Supervisión realizada por la Junta Directiva
- Supervisión realizada por el Comité de Auditoría
- Línea ética
- Asignación de autoridad y responsabilidad
- Programas de autoevaluación
- Políticas que abordan las prácticas importantes de control del negocio y administración del riesgo

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 34 de 55
		Versión: 02
		Fecha: 01/06/2020

#### 12.4. CONTROLES GENERALES DE TECNOLOGÍA DE LA INFORMACIÓN (ITGC)

En el proceso de evaluación de los riesgos relacionados con el reporte financiero, se debe obtener un entendimiento de cómo la Organización utiliza la tecnología de información y como ésta afecta los reportes financieros. En especial, porque son importantes para la efectividad de los controles automáticos; es decir, aseguran que estos funcionen sobre sistemas de información, aplicaciones y/o bases de datos seguros.

Para la evaluación de estos controles, Grupo Aval definió como marco de referencia los "Controles Generales de Tecnología de la Información", enmarcados por las Normas Internacionales de Auditoría. Este marco establece los riesgos específicos de tecnología que afectan el control interno sobre reportes financieros en los siguientes dominios:

- **Accesos a programas y datos:** controles que buscan asegurar que solamente son otorgados accesos apropiados y autorizados sobre los sistemas y datos (passwords, firewalls, encriptación de datos, manejo de usuarios, privilegios de acceso sobre las aplicaciones o las funcionalidades de las aplicaciones).
- **Desarrollo y mantenimiento a los programas:** controles que buscan validar que los cambios a los programas y componentes de infraestructura tecnológica son solicitados, autorizados, desarrollados, probados e implementados, con el fin de lograr el cumplimiento de los objetivos de la Alta Dirección sobre los controles en los sistemas de información.
- **Operaciones computarizadas:** controles que buscan asegurar que los sistemas en producción procesan completa y adecuadamente, asimismo los problemas de procesamiento son identificados y resueltos adecuadamente para mantener la integridad de los datos financieros.

Si bien estos controles no están directamente relacionados con los riesgos de reporte financiero, el adecuado funcionamiento de un control automático o manual dependiente de TI depende de que los controles generales de TI sean efectivos.

#### 12.5. CONTROLES CLAVE PARA ORGANIZACIONES PRESTADORAS DE SERVICIO (OPS)

En caso de que la Organización cuente con organizaciones Prestadoras de Servicio (OPS), los dueños

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

de proceso deben implementar actividades de control tendientes a proteger la integridad, exactitud y validación de la información procesada, enviada y recibida de la OPS. Los procesos con impacto sobre el reporte financiero soportados por OPS, están sujetos a las mismas expectativas de control interno que aquellos ejecutados directamente por la empresa. Por lo anterior, la Organización debe obtener un reporte ISAE 3402 Tipo II o velar por la ejecución de pruebas de auditoría realizados por la Organización sobre el tercero o por el reprocesamiento de las actividades clave de control ejecutadas por la OPS.

Para aquellas actividades realizadas por las OPS consideradas como parte del control interno sobre el reporte financiero, se deben realizar uno de los siguientes procedimientos, en su orden:


1. Obtener un informe ISAE 3402 Tipo II y evaluar el resultado de la validación de los controles del tercero sobre las actividades realizadas por este.

Si el informe se emite por un periodo evaluado inferior a 6 meses y/o con corte anterior a 3 meses de acuerdo con la fecha de reporte de Grupo Aval (es decir, un reporte con fecha de corte anterior al 1 de octubre), es necesario solicitar a la Organización Prestadora de Servicios, una certificación por el periodo descubierto (hasta la fecha de corte de los Estados Financieros de la Organización), la cual debe ser emitida por el Auditor que emitió el informe ISAE 3402 Tipo II, indicando el resultado de la evaluación realizada para dicho periodo. Esta certificación se conoce con el nombre de "Gap Letter" o "Bridge Letter".

Si el periodo evaluado fue de mínimo 6 meses y la fecha de corte está dentro de los 3 meses anteriores a la fecha de cierre del reporte financiero de la Organización (esto es, entre el 1 de octubre y el 31 de diciembre), se deberá solicitar una comunicación a la OPS para poder obtener evidencia respecto a los controles evaluados, para determinar que estos continuaron operando tal y como se diseñaron desde la fecha de corte del ISAE hasta el 31 de diciembre.

2. Si el tercero no emite un reporte ISAE 3402 Tipo II, realizar una prueba de controles en el tercero: si el contrato con el tercero tiene una cláusula de "derecho de auditoría", que le permita a la entidad contratante realizar auditorías al tercero, a través de la función de Auditoría Interna, quien revisará y probará los controles ejecutados por el tercero.

3. Obtener un reporte de aplicación de procedimientos previamente convenidos que describa las

	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 36 de 55
		Versión: 02
		Fecha: 01/06/2020

pruebas realizadas sobre los controles relevantes. Este reporte puede ser utilizado para proveer evidencia similar a la de un reporte ISAE 3402 Tipo II. En tal caso la administración debe evaluar que este reporte incluya:

- Los controles del tercero que son relevantes para el control interno sobre reporte financiero en la organización y que cubra los cinco componentes de control interno.
- El periodo cubierto en la evaluación, la naturaleza y los resultados de las pruebas realizadas por el auditor a los controles para validar que operen efectivamente.

Como medida final y en caso de que no fuera factible algunas de las opciones indicadas en los párrafos anteriores, el dueño del proceso debe identificar, o implementar de ser necesario, los controles suficientes para validar la calidad de estos (inputs), prevenir o detectar errores o fraude en la información financiera procesada y/o reportada por el proveedor e incluirlos en la matriz SOX para que surtan el proceso de evaluación.


La documentación de las conclusiones sobre el análisis del reporte proveído por la OPS sobre la efectividad y suficiencia de los controles, y los ejecutados por la entidad contratante sobre el mismo proceso, deben documentarse en el formato Memorando de Conclusión – Organizaciones Prestadoras de Servicios. Estas conclusiones deben estar alineadas con los controles ejecutados por la OPS y por la Organización, en concordancia con el entendimiento propio del proceso, con el fin de que se dé cobertura apropiada a los riesgos aplicables.

## 12.1. CONTROLES CLAVE EN PROCESOS TERCERIZADOS A CENTROS DE SERVICIO COMPARTIDOS (CSC)

Anualmente, durante el primer bimestre y para efectos de determinación del alcance SOX, cada Organización bajo alcance SOX debe analizar si ha tercerizado (o tiene proyectado tercerizar) algún proceso que tenga impacto SOX (registro contable, generación de información financiera, ejecución de controles clave SOX, entre otros) a otra Subordinada del Grupo (Centro de Servicios Compartidos o CSC).

En caso de identificar algún CSC, la Organización deberá informarlo a casa matriz detallando la entidad considerada como un CSC, la entidad usuaria y el proceso tercerizado con impacto en SOX. Así mismo, durante el proceso de actualización de la evaluación cualitativa que se surte en el segundo semestre de cada año, la Organización deberá evaluar si existe algún CSC nuevo para evaluar su impacto.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 37 de 55
		Versión: 02
		Fecha: 01/06/2020

Cada entidad usuaria deberá, en coordinación con el CSC, definir el flujo del proceso o modelo operativo que permita identificar, tanto al CSC como a la entidad usuaria, los controles clave SOX asignados en cada una de las partes y que son necesarios para mitigar los riesgos asociados al proceso tercerizado. Estas responsabilidades establecidas entre las partes deberán ser parte integral de los Contratos o Acuerdos de Servicio.

El CSC y la entidad usuaria, deberán incluir los controles en la matriz de riesgo control clave respectiva, en las fechas que corresponda y deberá ejecutar los controles con frecuencia, oportunidad y calidad para mitigar apropiadamente los riesgos. Dichos controles deben reflejarse en la Matriz Sox de la entidad que los ejecuta y, por lo tanto, no deben estar duplicados en las matrices de ambas entidades.

De acuerdo con las pruebas de Auditoría Interna Fase 1 y Fase 2, respectivamente, cada CSC deberá emitir un memorando de conclusión dirigido a cada entidad usuaria, indicando el resultado de las pruebas de diseño y efectividad de los controles probados por la Auditoría Interna, detallando el resultado de la evaluación realizada para cada control SOX. Este memorando se deberá realizar de manera oportuna con el fin de que las entidades usuarias identifiquen controles compensatorios, en caso de ser necesario para mitigar los riesgos asociados en los procesos.

Los controles inadecuados e inefectivos deben ser cuantificados y reportados en el Reporte de Deficiencias de Control (RDC) y Tablero de Control.

## 12.2. CONTROLES SOBRE ARCHIVOS ELECTRÓNICOS (ADUS)


Los dueños de proceso deben asegurar las Aplicaciones Desarrolladas por el Usuario (ADUs) que soporten controles incluidos en la matriz SOX de los procesos a su cargo y que tengan impacto sobre el reporte financiero. Lo anterior, para apoyar que los controles operen de manera efectiva para prevenir o detectar errores o fraudes sobre los estados financieros, y asegurar que:

- Las modificaciones sobre las ADUs no afecten la integridad de la información y precisión de los cálculos manejados a través de estas.
- Solamente se haga uso de versiones de ADUs aprobadas.
- Los datos que se administran a través de las ADUs se aseguran de manera apropiada.
- Los datos alimentados en las ADUs se ingresan de manera completa y exacta.

Las actividades para ejecutar por los dueños de proceso como parte de la identificación y aseguramiento de ADUs se describen a continuación.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 38 de 55
		Versión: 02
		Fecha: 01/06/2020

### 12.2.1. Listar las ADUs que soportan controles SOX

El dueño de proceso debe realizar una revisión de los controles a su cargo dentro de la Matriz SOX, identificando todas las ADUs que se utilizan en la ejecución de estos. Las ADUs identificadas deben incluirse en el inventario de ADUs en el formato establecido por Grupo Aval "Inventario, Análisis y Monitoreo ADUs", el cual debe ser diligenciado de manera completa y exacta con el apoyo del equipo SOX.

### 12.2.2. Clasificar las ADUs según su tipo de uso

Una vez se cuenta con el inventario, se requiere identificar las ADUs críticas para el reporte financiero. Para ello, se deben clasificar las ADUs en operacionales, analíticas y financieras con base en los siguientes criterios:


**Operacionales:** Listados, reportes de diferentes fuentes, listas de chequeo, conciliaciones y cualquier otra información que se genera como evidencia electrónica de algún tipo de seguimiento o monitoreo, que apoyan la ejecución de un control en la Matriz SOX, pero sus salidas no generan cifras que afecten los estados financieros.

**Analíticas:** ADUs que soportan la ejecución de controles marcados en la Matriz SOX de Riesgos - Control Clave SOX como "Control de Revisión de la Gerencia" y otros controles relacionados con revisiones analíticas, para evaluar la razonabilidad de los montos financieros o cualquier análisis cuantitativo o matemático, para determinar la razonabilidad de las transacciones o partidas incluidas en los reportes financieros. Por ejemplo, análisis de variaciones, análisis de tendencias e indicadores, recálculos de verificación, entre otras.

**Financieras:** ADUs que determinan los montos o valor de las transacciones que se registran en los estados financieros, como la determinación de provisiones, estimaciones, soporte de ajustes manuales en la contabilidad, entre otros.

Las ADUs que se clasifiquen como **Analíticas** o **Financieras** se consideran como ADUs SOX, para éstas se deben implementar los criterios de aseguramiento que se establecen en el siguiente numeral. Las ADUs que se clasifiquen como Operacionales no se consideran ADUs SOX, por lo tanto, no se requiere

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 39 de 55
		Versión: 02
		Fecha: 01/06/2020

la implementación de los parámetros de aseguramiento sugeridos.

### 12.2.3. Implementar controles de aseguramiento sobre ADUs SOX

Los controles mínimos para el aseguramiento de las ADUs SOX Analíticas o Financieras son los siguientes:


- a. **Control y autorización de cambios:** proceso controlado de cambios para asegurar que se mantiene el historial de las modificaciones asociadas con la lógica de las rutinas, fórmulas, macros o inputs que afecten estimaciones en las ADUs SOX, y que tales cambios se aprueban por el nivel jerárquico que tenga atribución; así mismo, el control de cambios y autorizaciones ayuda al dueño de proceso a asegurar que está en uso la última versión aprobada.

Como buena práctica se pueden definir convenciones para el nombre de los archivos y la estructura de los directorios en donde estos se almacenan, incluir en el historial de cambios la fecha del cambio, la modificación realizada, el estamento que la aprobó y el nombre o número de la versión oficial

- b. **Control de acceso (crear, leer, editar, eliminar):** limitar el acceso a las ADUs almacenándolas en un servidor central o equipos propios del colaborador a cargo de la ejecución del control con el debido aseguramiento de carpetas compartidas y asignando el acceso a dicha ubicación al personal apropiado. Así mismo, se debe asignar contraseña para restringir el acceso.
- c. **Seguridad de los datos:** implementar un proceso para asegurar que la formulación de la ADU así como su resultado final, no sean modificados, lo cual puede realizarse "bloqueando" o protegiendo celdas o datos para prevenir cambios inadvertidos o intencionales. Es importante que, para esta actividad de control, el dueño de proceso defina las celdas de formulaciones que deben estar protegidas teniendo en cuenta las celdas críticas.
- d. **Respaldo:** implementar un proceso de respaldo periódico de las ADUs de tal forma que, para propósitos de reporte financiero externo, esté disponible la información completa. Es importante para esta actividad de control identificar los medios de respaldo y las áreas o colaboradores encargados de la custodia de estas.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 40 de 55
		Versión: 02
		Fecha: 01/06/2020

Existen ADUs que soportan cálculos complejos, valoraciones o sirven como herramienta para la preparación o ejecución de modelos, las cuales se caracterizan comúnmente por el uso de macros y múltiples hojas de soporte donde se vinculan celdas, valores y hojas de trabajo individuales; para este tipo de ADUS, además de los controles anteriores, se deberán implementar las siguientes medidas de aseguramiento:

- e. **Documentación:** asegurar que se mantiene el nivel apropiado de documentación actualizada de la ADU para entender el objetivo y las funciones específicas de la misma. Es importante para esta actividad de control asegurar que, durante el proceso de cambio y mantenimiento de la ADU, se actualizan permanentemente estos documentos como fuente básica de soporte.
- f. **Inspección lógica:** alguien diferente a quien programó la ADU debe verificar que los cambios relacionados con la lógica de las rutinas, fórmulas, macros o inputs genéricos que afecten estimaciones, funcionan como se espera, preservando la integridad y exactitud de la ADU. Esta verificación se puede realizar por ejemplo a través de análisis de razonabilidad de los resultados obtenidos frente a los cambios aplicados, ratificando de esta manera que la ADU funciona de la manera como se diseñó.

Cuando técnicamente no se pueda implementar alguno de los controles sugeridos o el análisis de costo beneficio lleve a concluir que no es eficiente la implementación de alguno de estos controles, esto debe documentarse formalmente como una excepción dentro del inventario de ADUs indicando las razones por las cuales el aseguramiento no es posible, describiendo cómo se mitiga el riesgo de pérdida de la integridad y exactitud de la información procesada a través de la ADU SOX, junto con la aprobación por parte del Director del Área según corresponda.


#### 12.2.4. Mantenimiento del Inventario de ADUs SOX

Cada vez que se modifiquen los controles relacionados en la matriz SOX, el dueño de proceso con el apoyo del Oficial SOX de la Organización, será responsable de asegurar que:

- Todo cambio (adición o modificación) sobre los controles SOX involucre también la identificación de nuevas ADUs SOX.
- Actualización del inventario de ADUs, según corresponda.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------



 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 41 de 55
		Versión: 02
		Fecha: 01/06/2020

- Aseguramiento de nuevas ADUs de acuerdo con los lineamientos establecidos.

Este inventario debe ser revisado mensualmente para asegurar su exactitud.

### 12.3. CONTROLES EN PROCESOS DE MIGRACIÓN

Todas las entidades enfoque 1 deben incluir los controles SOX asociados al proceso de migración, en cambio las entidades enfoque 2, deberán incluir los controles en el evento en que se presenten dichos procesos, asociados al proceso impactado por el cambio. Para el efecto, se deberán considerar los riesgos SOX referentes a migración, establecidos en el Inventario de Riesgos Genéricos y se deberá evaluar la aplicación de los siguientes controles clave, para que sean incorporados en la Matriz SOX:

- Análisis y diseño del proceso de migración/conversión de datos
- Gestión de errores durante el proceso de conversión/migración
- Ejecución y certificación de pruebas de usuario previo al paso a producción
- Aprobación de los dueños de proceso previo al paso a producción
- Validación y certificación de datos en el ambiente productivo
- Validación y certificación de datos ingresados manualmente
- Aseguramiento del ambiente de producción
- Controles de conciliación entre sistemas

### 12.4. CONTROLES DE REVISIÓN DE LA GERENCIA (MRC)

Los controles de revisión de la gerencia involucran a miembros de la Presidencia, Vicepresidencias o Direcciones con el fin de analizar, revisar y/o evaluar sobre ciertas actividades y controles desarrollados por otros colaboradores y concluir sobre la información financiera, gestión y/o resultados.

Este tipo de revisiones incluyen, por ejemplo, seguimiento presupuestal, análisis de indicadores de gestión, reporte de variaciones, reportes de excepción, revisión de la razonabilidad de los estados financieros, cálculos globales sobre balances y revelaciones y reportes que contienen estimaciones o juicios.

Los controles de revisión de la gerencia generalmente cumplen con las siguientes características:

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

- El control involucra miembros de la Alta Dirección y otros colaboradores con apropiado conocimiento, quienes revisan la información de reportes, resúmenes ejecutivos, registros de excepción y otra información preparada por la Organización con el fin de llegar a una conclusión sobre el reporte financiero.
- La ejecución de estos controles requiere por lo menos, un moderado grado de juicio de la persona que realiza la revisión.
- Estos controles normalmente están relacionados con estimaciones contables y/o transacciones inusuales.
- El control regularmente sirve como mecanismo de monitoreo para verificar la efectividad operativa de otros controles de más bajo nivel asociados con el aseguramiento de la razonabilidad de los datos sujetos a revisión.

#### 12.4.1. Documentación de controles MRC

El apropiado diseño de los controles MRC incluye la definición de métricas, umbrales de tolerancia, señales de alerta y otros criterios, así como otros controles relacionados para determinar cómo la administración se asegura que el control opere y con qué grado de precisión, de acuerdo con sus objetivos de control.

El equipo SOX de la Organización debe apoyar a los dueños de proceso en la identificación de los controles MRC y en el aseguramiento de la documentación correspondiente. No obstante, es responsabilidad de los dueños de proceso, en este caso, Alta Dirección, velar por que sus controles MRC se encuentren documentados adecuadamente.

La necesidad de una adecuada documentación es relevante en el marco COSO 2013, el cual establece la importancia de asegurar la documentación de los controles por parte de la Gerencia considerando el proceso de juicio aplicado en la gestión y análisis. Dado que la sola firma en un documento ofrece poca o ninguna evidencia por sí misma acerca de la eficacia del control MRC, se requiere contar con la documentación robusta en aquellas áreas o controles en donde el juicio es más significativo, de tal manera que la Alta Dirección documente las consideraciones más importantes, cómo se toman las decisiones y cómo se llega a las conclusiones.

Una documentación robusta de los controles MRC debe incluir los siguientes aspectos:


Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

Código: DG-0106/2

- **Objetivo del control:** propósito de la revisión para la cual se está ejecutando el control. El objetivo del control debe tener una relación lógica con el riesgo que se desea mitigar y debe estar alineado con el desarrollo documentado en la evidencia y en las conclusiones de este.
- **Fuente:** de donde proviene la información objeto de revisión del MRC y la fecha de corte.
- **Nivel de precisión:** nivel de desagregación o de detalle con el cual se hace el análisis de la información alineado con el objetivo del control.
- **Frecuencia:** periodicidad y momento en el cual se ejecuta el control alineado con su objetivo.
- **Cuentas contables/aserciones asociadas:** cuentas contables o aserciones sujetas a revisión.
- **Umbral de tolerancia:** dato o parámetro a partir del cual se considera que las cifras analizadas podrían presentar un comportamiento inusual o inesperado y que requieren seguimiento o investigación adicional. Este umbral de tolerancia debe estar debidamente justificado.
- **Descripción de la revisión efectuada:** detalle del análisis, juicios y consideraciones realizados por el responsable del control, considerando los aspectos del MRC mencionados anteriormente.
- **Investigación / profundización:** la Alta Dirección, alineada con los umbrales definidos, identifica variaciones, excepciones, diferencias, errores, cuentas o comportamientos inusuales fuera de los umbrales definidos en el control y establece canales y procedimientos de investigación y/o profundización con el fin de descartar cualquier error en el reporte financiero, asegurando:
- **Acciones correctivas:** documentar si los errores o diferencias fueron investigados y si se tomaron acciones correctivas, concluyendo si los resultados obtenidos son satisfactorios de acuerdo con sus expectativas.

## 12.5. REUBICACIÓN DE CONTROLES QUE NO SON CLAVE PARA SOX

Los controles SOX que no sean considerados como clave para el reporte financiero, deben ser reubicados en otra matriz de riesgo que corresponda. La reubicación de los controles se puede generar

	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 44 de 55
		Versión: 02
		Fecha: 01/06/2020

por:

- a. **Eliminación de contenido clave por cambios en procesos:** cuando la organización cambia la manera en que opera el proceso, puede ocurrir que los riesgos y controles previamente identificados no sean vigentes y por lo tanto se hace necesario eliminarlos de la Matriz SOX.
  
- b. **Reubicación de controles en otras matrices de riesgo:** La implementación de líneas base de controles, controles de revisión de la gerencia y el grado de madurez del Sistema de Control Interno conllevan a que se reevalúe la suficiencia de los controles y se identifique algunos controles transaccionales que ya no se consideren clave para SOX. En estos casos, se debe seguir los siguientes parámetros:
  - **Actualización del Inventario de Riesgos SOX:** Anualmente y durante el primer trimestre del año, Grupo Aval expide el Inventario actualizado de Riesgos SOX vigente para cada ejercicio. Es usual que, por diferentes razones como la optimización de los procesos, cambios en la industria o mercado, entre otros, se eliminen o consoliden algunos riesgos SOX. En estos casos, los equipos SOX deben evaluar con los dueños de proceso, si los controles asociados a dichos riesgos deben ser reasignados a otros sistemas de administración de riesgo (por ejemplo, riesgo operativo) y continuar vigentes o si, por el contrario, tales controles ya no son considerados clave ni para el proceso SOX, ni para otros riesgos. En estos casos, el dueño de proceso, junto con el equipo SOX proceden a hacer la eliminación y documentación respectiva en el control de cambios de la Matriz SOX.
  
  - **Implementación de Controles de Revisión de la Gerencia (MRC):** Cuando en un proceso se identifique un control de alto nivel (MRC), es responsabilidad del equipo SOX y del dueño de proceso correspondiente, evaluar el nivel de precisión de este para determinar qué controles adicionales son requeridos para mitigar el riesgo de cara a las aserciones impactadas. Como resultado de esta evaluación, podrían identificarse controles que ya no deberían ser considerados como clave para el proceso, siendo necesario que estos controles sean "Reubicados" en matrices de riesgo-control diferentes a SOX. En tal caso los equipos SOX elevarán consulta a su casa matriz directa, para que el equipo Corporativo SOX defina la viabilidad de su reubicación. En caso de una respuesta afirmativa, el equipo SOX de la Organización debe preparar la documentación del control de cambios

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

respectivo y verificar que el control sea incluido en la matriz que corresponda. En ningún caso esto implica que el control deje de ser ejecutado por parte del dueño de proceso.

- **Autoevaluación de la suficiencia de los controles:** cuando se llegue a identificar un control operativo o de otra naturaleza que no sea clave para SOX, esta situación deberá ser notificada por el dueño de proceso al Oficial SOX de la entidad matriz directa y este a Grupo Aval, para que estudien si procede su reubicación en las matrices que se sugieran (SARO, Anticorrupción, etc.) y será desmarcado como clave de la matriz SOX; en cuyo caso Grupo Aval deberá confirmar por correo electrónico al área SOX de la organización si procede el cambio para que dicha área confirme a su vez que el control fue reasignado y a cual matriz.

En todos los casos se debe garantizar a la tercera línea de defensa y al auditor externo, un claro y detallado análisis en el control de cambios que acompaña los cambios mensuales en las matrices, sobre la justificación de su eliminación o reubicación. Si en concepto de cualquiera de tales instancias (tercera línea de defensa y/o Auditoría Externa), el cambio sugerido va en detrimento del aseguramiento del Sistema de Control a la Información Financiera, deberá procederse de manera inmediata a revertir dicha reubicación de los controles.

Para identificar controles que eventualmente requieren reubicación por ser considerados no clave para SOX, pueden considerarse los siguientes aspectos:


- Cuando un riesgo se encuentre cubierto por una alta cantidad de controles, en comparación con el promedio de los demás riesgos, puede ser una señal de que cada uno de los controles individuales no son lo suficientemente fuertes y deberá adelantarse el análisis frente al impacto del riesgo en las aserciones de la cuenta contable relacionada. En tal caso, se debe evaluar si existen otros controles de mayor nivel que permiten reemplazar algunos de los ya identificados.
- Existen algunos controles que pueden ser catalogados a la vez como SARO, SOX o Anticorrupción, entre otros. Sin embargo, los controles clave para SOX son de Alto Nivel y por lo general, no responden a las condiciones de riesgo operativo u otros.
- Como parte del proceso de maduración, se debe velar por que los controles clave estén concentrados en controles automáticos y controles de alto nivel y, en una menor proporción, en

controles transaccionales. Dicha definición depende del grado de cobertura que los controles den al riesgo desde la perspectiva de la aserción.

- La mezcla entre controles de alto nivel y controles transaccionales está dada por el cubrimiento que los primeros den al riesgo y a las aserciones de la cuenta contable relacionada. Es usual que controles de Alto Nivel con niveles de precisión apropiados, den cobertura a aserciones como Valuación, y muy poco a Existencia, por lo que es natural que para esta última se cuente con controles a nivel de transacción.
- Los controles automáticos siempre serán más eficientes que los controles manuales y es usual que los primeros reemplacen satisfactoriamente a otros transaccionales que podrían coincidir con controles de riesgo operativo o de otra naturaleza.
- Los controles manuales centralizados son más robustos que los controles automatizados debido a la mayor probabilidad de falla que presentan. Normalmente, controles manuales en cabeza de múltiples dueños de proceso o que operan en múltiples localidades tienden a ser controles operativos o transaccionales. Este tipo de controles pueden ser reemplazados por otros centralizados que abarquen las mismas aserciones y que sean ejecutados por un nivel jerárquico más alto. La calificación del "Nivel de Atención Requerido – NAR" es una buena fuente de información para identificar aquellos riesgos en donde existen controles manuales, descentralizados, que pueden ser sujetos a análisis, para determinar si existe otro tipo de control más robusto que lo reemplace dentro de las matrices SOX.
- Al analizar cada uno de los riesgos se deberá tener en consideración los controles de más alto nivel y los automáticos frente a la cobertura en función de las aserciones. Cuando alguna aserción quede descubierta de cara al riesgo, se irán requiriendo más controles de menor nivel (manuales u operativos) hasta dar la cobertura con la que la administración logre identificar errores significativos de forma oportuna.

## 12.6. EFICACIA OPERATIVA

Los dueños de proceso son responsables de ejecutar de forma uniforme y permanente los controles clave a su cargo, así como de documentar de forma completa, suficiente y exacta la evidencia que soporta la ejecución de estos, con el fin de demostrar la forma en que llevó a cabo el control (de

 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 47 de 55
		Versión: 02
		Fecha: 01/06/2020

acuerdo con el tipo y naturaleza del mismo), la oportunidad con la que lo ejecutó y las conclusiones obtenidas, entre otros factores. Asimismo, es importante que documente la confirmación de la fuente de información antes de ejecutarlo, la actividad de control realizada, tratamiento de excepciones y otros aspectos que considere relevantes en la ejecución del control.

La evidencia de la ejecución de los controles debe estar siempre disponible para cualquier revisión (auditores internos, auditores externos, revisiones cruzadas, auto revisiones, etc.). Lo anterior, no implica que toda la evidencia se encuentre en medio físico (impresa), dado que puede documentarse y conservarse de forma electrónica (correo electrónico, archivos de Excel, Access, logs y registros del sistema, workflow de aprobaciones, etc.) siempre y cuando se mantengan implementados controles que aseguren que la información no sea modificada (formulación, parametrización o datos).

La evidencia debe mantenerse ordenada, completa y archivada de tal forma que siempre pueda ser suministrada para revisión de manera oportuna. La custodia de la evidencia de ejecución del control es del dueño de proceso, quien debe velar por que la organización cuente con mecanismos apropiados de archivo que le permitan tener disponible la información por el tiempo mínimo que exige la ley local.

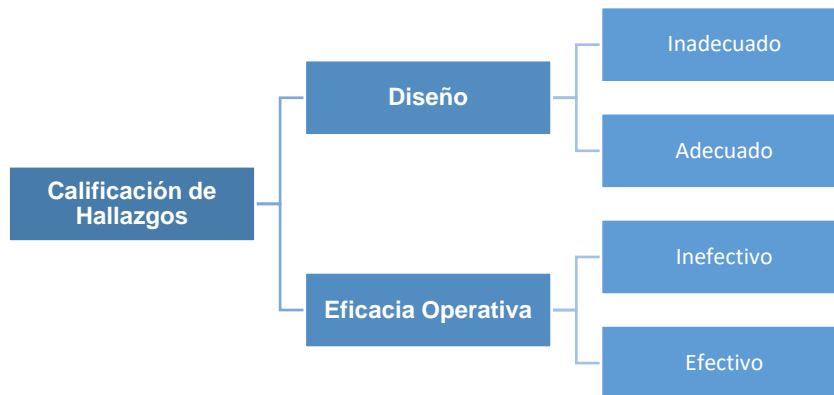
### 13. EVALUACIÓN DE CONTROLES

La Auditoría Interna, de acuerdo con el cronograma de trabajo establecido, realiza las pruebas de diseño y eficacia operativa de los controles definidos por los dueños de proceso, con base en la Matriz SOX, Inventario de ADUs e Inventario de aplicaciones reportadas por el Oficial SOX de la Organización.

Cada vez que se evalúa el diseño y la eficacia operativa de los controles, el Auditor Interno presenta a la Vicepresidencia Financiera y Administrativa o quien haga sus veces, a los dueños de proceso y al Oficial SOX de la Organización los hallazgos identificados, indicando la conclusión de sus pruebas de diseño y de eficacia operativa con el detalle de los hallazgos identificados.

La siguiente es la clasificación de los hallazgos, de acuerdo con los resultados de las pruebas de auditoría interna:

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------



Los controles calificados como adecuados son sujetos a pruebas de eficacia operativa por parte de la Auditoría Interna. Un control calificado como inadecuado deberá ser remediado de manera oportuna con el fin de que se efectúen las pruebas de eficacia operativa y así poder concluir que el riesgo está siendo mitigado.

### 13.1. REMEDIACIÓN, EVALUACIÓN Y CLASIFICACIÓN DE DEFICIENCIAS

Si dentro de las revisiones independientes realizadas por la auditoría (interna o externa) se identifican controles inadecuados o inefectivos, el dueño de proceso debe:

- Definir si el control requiere ajustes en su diseño o si se debe identificar un control compensatorio para mitigar el riesgo.
- Informar y acordar con el Oficial SOX los ajustes a los controles existentes o el diseño de los nuevos controles a incluir en la Matriz.
- Implementar los ajustes en las Políticas y/o procedimientos asociados al proceso.
- Garantizar que los planes de remediación sean los apropiados para atender los hallazgos de las evaluaciones independientes.

Para ello el equipo SOX debe:

- Apoyar al dueño de proceso en el entendimiento de la falla de diseño (Inadecuado) o de la falla operativa (Inefectivo), y, de ser necesario, apoyarlo en brindar explicaciones adicionales al revisor independiente (Auditor Interno o Externo).
- Apoyar al dueño de proceso en la identificación de los ajustes al control ya sea modificación por



cambio en el control o en la identificación de otro control.

- Sugerir al dueño de proceso la redacción de la modificación o del nuevo control identificado, en la respectiva Matriz SOX.
- Apoyar al dueño de proceso en la actualización de la Matriz SOX respectiva de acuerdo con lo definido y en la documentación del control de cambios, asegurando que se mantenga el historial en la Matriz SOX, indicando hasta qué fecha operó el control anterior y desde cuándo funciona el nuevo control o el cambio aplicado.

### 13.2. EVALUACIÓN Y CLASIFICACIÓN DE DEFICIENCIAS AL CIERRE DEL EJERCICIO

Una vez finalizado el ejercicio anual para el cumplimiento con la Ley SOX, las deficiencias de control interno sobre reporte financiero informadas por los Auditores Internos deben ser evaluadas y clasificadas con el ánimo de determinar si de manera individual o combinada, corresponden a debilidades significativas o materiales que tengan un efecto en el manifiesto o certificación anual de control interno sobre reporte financiero emitida a casa matriz.

Para ello se requiere documentar adecuadamente los criterios y conclusiones del análisis realizado de manera que cualquier órgano de control pueda llegar a la misma conclusión. Por lo anterior, el análisis realizado para cada una de las deficiencias de control debe ser documentado de manera íntegra, exacta y oportuna en el formato de Reporte de Deficiencias de Control (RDC) establecido por Grupo Aval.

Las deficiencias o un grupo de ellas pueden clasificarse en:

**Deficiencia de Control:** es una ausencia o insuficiencia en el diseño u operación de un control, que no permite a la Alta Dirección o a los dueños de proceso detectar o prevenir errores en los estados financieros de manera oportuna durante el normal desarrollo de sus funciones.

**Deficiencia Significativa:** es una deficiencia o combinación de deficiencias de control interno que indican la existencia de una “posibilidad razonable” de que un error en los estados financieros, que esté por debajo del nivel de materialidad, no sea prevenido o detectado, afectando adversamente la habilidad para iniciar, autorizar, contabilizar, procesar o reportar información financiera.

**Debilidad Material:** es una deficiencia o combinación de deficiencias de control interno que indican la

existencia de una “posibilidad razonable” de que un error en los estados financieros, por encima o muy cercano al nivel de materialidad, de tal forma que no sea prevenido o detectado, afectando adversamente la habilidad para iniciar, autorizar, contabilizar, procesar o reportar información financiera.

Esta clasificación se realiza con base en:


- Probabilidad de ocurrencia de un error en los estados financieros como consecuencia de la deficiencia identificada.
- El impacto financiero residual, el cual se identifica una vez se han evaluado los controles compensatorios y otros factores que pueden afectar la probabilidad de ocurrencia.

Cuando se tienen múltiples deficiencias que afectan una misma cuenta contable o revelación, se incrementa la probabilidad de error sobre el estado financiero, por lo un grupo de deficiencias en conjunto podría llegar a representar una deficiencia significativa o debilidad material. Por lo anterior, el Oficial SOX de la organización debe adelantar un análisis consolidado de deficiencias a nivel de cuentas contables, relevaciones o componentes de control interno afectados, con el fin de determinar si colectivamente estos representan una deficiencia significativa o debilidad material.

La relación entre la clasificación de la deficiencia y la probabilidad de ocurrencia e impacto financiero residual es la siguiente:

Clasificación de la Deficiencia	Probabilidad de Ocurrencia	Impacto Financiero Residual
Debilidad material	Razonablemente posible o probable, y	Superior al 5% de la utilidad antes de impuestos
Debilidad significativa	Razonablemente posible o probable, y	Entre el 1% y 5% de la utilidad antes de impuestos
Deficiencia de control	Remota, o	Inferior al 1% de la utilidad antes de impuestos

Asimismo, se debe analizar si la reincidencia de deficiencia puede implicar que no sean identificados oportunamente errores materiales en el reporte financiero, en cuyo caso podría cambiar la clasificación de la deficiencia.


 <b>PROINDESA</b>	<b>POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</b>	Página 51 de 55
		Versión: 02
		Fecha: 01/06/2020

Este mismo análisis agregado debe ser realizado considerando la existencia de debilidades identificadas a nivel de los componentes del entorno de control, entre las cuales se destacan:

- Actualización de los estados financieros emitidos para realizar ajustes sobre cifras y/o declaraciones erróneas. Este aspecto no abarca las actualizaciones realizadas para reflejar cambios sobre los principios contables con el fin de cumplir con nuevos requerimientos contables o cambios voluntarios de un principio contable generalmente aceptado a otro.
- Identificación de la existencia de un error material en los estados financieros en el período actual por parte del auditor, que no fue identificado inicialmente por las actividades de control establecidas en la organización.
- La supervisión de la información financiera de la organización y el control interno sobre la información financiera por parte del Comité de Auditoría de la organización no es efectivo.
- La función de Auditoría Interna o la función de la evaluación de riesgos no es efectiva.
- Identificación de fraude que involucre a miembros de la Alta Dirección, independiente de su cuantificación.
- Deficiencias significativas que han sido comunicadas a la Presidencia y al Comité de Auditoría, y permanecen sin corregir después de dos periodos contables consecutivos. Lo anterior, a menos que se trate de deficiencias que solo puedan ser remediadas a través de la implementación de nuevas aplicaciones o cambios sobre las existentes y que requieran un periodo más largo para ponerlas en funcionamiento.

Cuando se trata de segregación de funciones y accesos, es necesario identificar las aplicaciones, bases de datos o sistemas operativos, así como los módulos, submódulos y transacciones afectadas para poder identificar la cuenta contable impactada. Se debe determinar el monto expuesto y hacer la respectiva revisión de los logs que permitan concluir si se materializó el riesgo por uso inadecuado de acceso o por conflicto en la segregación de funciones, para poder cuantificar el impacto final. Si la falla se origina por desactualización de las matrices de roles y perfiles, sólo se debe proceder a su actualización y no requiere revisión de roles. Igualmente se debe hacer la cuantificación respectiva cuando se trate de fallas de controles relacionados con cambios en bases de datos.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.	<b>Código: DG-0106/2</b>
--	--------------------------

	<p style="text-align: center;">POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</p>	Página 52 de 55
		Versión: 02
		Fecha: 01/06/2020

## 14. INFORMACIÓN Y COMUNICACIÓN

### 14.1. REPOSITORIO DE INFORMACIÓN

La Organización cuenta con un repositorio de información en el cual se custodia la información SOX y la gestión realizada para el cumplimiento de la presente Política. Con lo anterior se garantiza la disponibilidad, oportunidad y confiabilidad de la información en caso de sea requerida por la Alta Dirección, dueños de proceso, equipo SOX de casa matriz u órganos de control (internos o externos).

### 14.2. CAPACITACIÓN

El Oficial SOX de la Organización, es responsable de velar por que se haga un empalme adecuado y oportuno a colaboradores nuevos del equipo SOX, en caso de ausencia temporal o definitiva de otro colaborador. Asimismo, debe velar por que se realice una inducción sobre el cumplimiento de la Ley SOX a los colaboradores nuevos.

El equipo SOX de Grupo Aval realiza anualmente una capacitación general a todos los miembros nuevos de los equipos SOX de la Organización y mediante talleres de refuerzo con programación anual a la totalidad del equipo SOX.


Es responsabilidad del Oficial SOX de la Organización reportar a su casa matriz directa, las necesidades de capacitación de dueños de proceso y equipos SOX a más tardar durante el último trimestre del año, así como de informar oportunamente cambios en el equipo SOX.

### 14.3. REPORTES

Los siguientes son los reportes que debe efectuar la Organización para dar cumplimiento a la metodología SOX:

1. **Formato de justificación de aplicación de riesgos SOX**, de la Organización preparado y reportado por el Oficial SOX de esta.
2. **Matriz SOX, Inventario de ADUs e Inventario de Aplicaciones y Estadísticas de riesgos y controles**

<p>Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.</p>	<p><b>Código: DG-0106/2</b></p>
---	---------------------------------

	<p style="text-align: center;">POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)</p>	Página 53 de 55
		Versión: 02
		Fecha: 01/06/2020

SOX de la Organización, preparada y reportada por el Oficial SOX de esta.

3. **Análisis de Organizaciones Prestadoras de Servicios (OPS)** de la Organización, preparado y reportado por el Oficial SOX de esta.
4. **Memorando de actualización de alcance SOX** de la Organización, preparado por el Presidente y Vicepresidente Financiero de cada compañía o quien haga sus veces.
5. **Reporte de Deficiencias de Control (RDC)** de la Organización, preparado por el Oficial SOX de esta con los dueños de proceso, con el análisis y cuantificación de impactos de los controles calificados como inadecuados o inefectivos por parte de la auditoría interna. El análisis debe incluir si las deficiencias, de manera individual o agregada, corresponden a debilidades significativas o materiales que tengan un efecto en el manifiesto o certificación anual emitido por el Presidente y Vicepresidente Financiero y Administrativo o quienes hagan sus veces. Este reporte se presenta con la misma frecuencia con la cual, la Auditoría Interna presenta los resultados de las evaluaciones de efectividad en las diferentes fases.
6. **Tablero de Control SOX** de la organización, con los resultados de los indicadores definidos por Grupo Aval mediante Instrucción corporativa, los cuales se preparan con base en los reportes de Auditoría Interna con corte a las Fases I y II.
7. **Memorando de confirmación de matriz SOX** firmado por los dueños de proceso con corte al 31 de diciembre del año objeto de aseguramiento, con el fin de certificar que la matriz SOX representa el estado actual del control interno sobre el reporte financiero.
8. **Evaluaciones cualitativas** de la Organización preparados por el Vicepresidente Financiero y Administrativo y Director Financiero y de Planeación o Contador de la Organización o quienes hagan sus veces, con base en los estados financieros del año inmediatamente anterior.
9. **Manifiesto o Certificación anual de control interno sobre reporte financiero de Proindesa S.A.S.**, firmado por el Presidente y Vicepresidente Financiero y Administrativo, dirigido al Presidente y Vicepresidente Financiero de casa matriz, en la cual certifican el desarrollo de la metodología de cumplimiento SOX en la Organización, el resultado obtenido en la evaluación de controles SOX por parte de la auditoría interna y la disposición que la administración le ha dado a dichos resultados, de tal forma que pueda manifestar que el sistema de control interno sobre reporte

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

**Código: DG-0106/2**

financiero de la Organización es efectivo. El manifiesto o certificación anual, debe presentarse con el Reporte de Deficiencias de Control de Proindesa S.A.S. adjunto y las manifestaciones o certificaciones de control interno sobre reporte financiero de las sociedades de Infraestructura bajo alcance SOX.

10. **Informe de gestión u opinión del Revisor Fiscal** de las sociedades de Infraestructura (incluyendo sociedades administradas) que no están bajo alcance SOX.

11. **Opiniones del Revisor Fiscal y/o Auditor Interno sobre el control interno**, En la organización, información que es comunicada por parte del Revisor Fiscal y Auditor Interno y que debe ser remitida por el Oficial SOX a casa matriz.


Los reportes mencionados anteriormente, se deberán presentar en las fechas establecidas por Grupo Aval mediante instrucciones corporativas. En todos los casos, estos reportes, así como las evidencias que respaldan los controles SOX, deberán custodiarse por un período mínimo de cinco (5) años en el repositorio de información definido por la Organización.

## 15. DOCUMENTOS DE REFERENCIA

M-AR-SX-01 Manual Corporativo de Cumplimiento Ley SOX de Grupo Aval y sus formatos anexos

## 16. CONTROL DE CAMBIOS

VERSIÓN	FECHA	PRINCIPALES CAMBIOS EFECTUADOS
01	23/09/2019	Creación del documento
02	01/06/2020	Actualización general del documento.

 <b>PROINDESA</b>	POLITICA PARA EL CUMPLIMIENTO DE LA LEY SARBANES OXLEY (SOX)	Página 55 de 55
		Versión: 02
		Fecha: 01/06/2020

17. FIRMAS DE REVISIÓN Y APROBACIÓN

Elaborado por:	Revisado por:
DIRECTOR DE RIESGOS	VICEPRESIDENTE FINANCIERO Y ADMINISTRATIVO
Margarita Rosa Ramirez	Vanessa Garay Guzmán

APROBADO POR JUNTA DIRECTIVA SEGÚN CONSTA EN EL ACTA No.

Verifique que esta copia es la vigente consultando la información del Listado Maestro de Documentos. Si esta es una copia física, sin el sello de copia controlada en color rojo, se considera como copia no controlada. Todas las copias magnéticas se consideran No controladas.

Código: DG-0106/2