

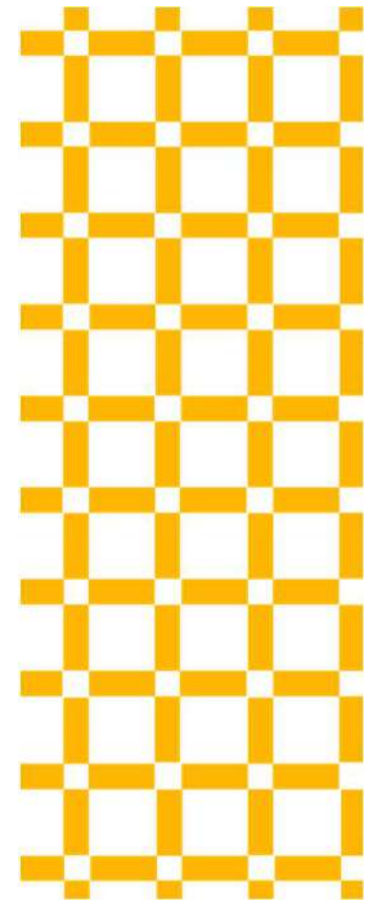
Impuesto sobre las Utilidades de las Empresas

Programa de Capacitación - ABAV
FY2020



Contenido

1. Marco Normativo
2. Sistemas de Imposición
3. Elementos Constitutivos
4. Principio de Fuente
5. Cálculo del Impuesto
6. Ajustes Tributarios
7. Tendencias de la A.I.T en Fiscalizaciones recientes
8. Prórrogas Tributarias
9. Ejercicio Práctico



1

Marco Normativo

Marco Normativo

LEY NRO. 843

LEY DE REFORMA TRIBUTARIA (20-05-1986)

TITULO III – IMPUESTO SOBRE LAS UTILIDADES DE LAS EMPRESAS

D.S. 24051

REGLAMENTO DEL IMPUESTO SOBRE LAS UTILIDADES DE LAS EMPRESAS (29-06-1995)

LEY NRO. 1606

- SUSTITUYE EL I.R.P.E.
- CREA EL I.U.E.

R.A. 05-0041-99

- AGRUPA TODAS LAS R.A. ANTERIORES Y VIGENTES

LEY NRO. 771

- CREA AA-IUE SECTOR FINANCIERO

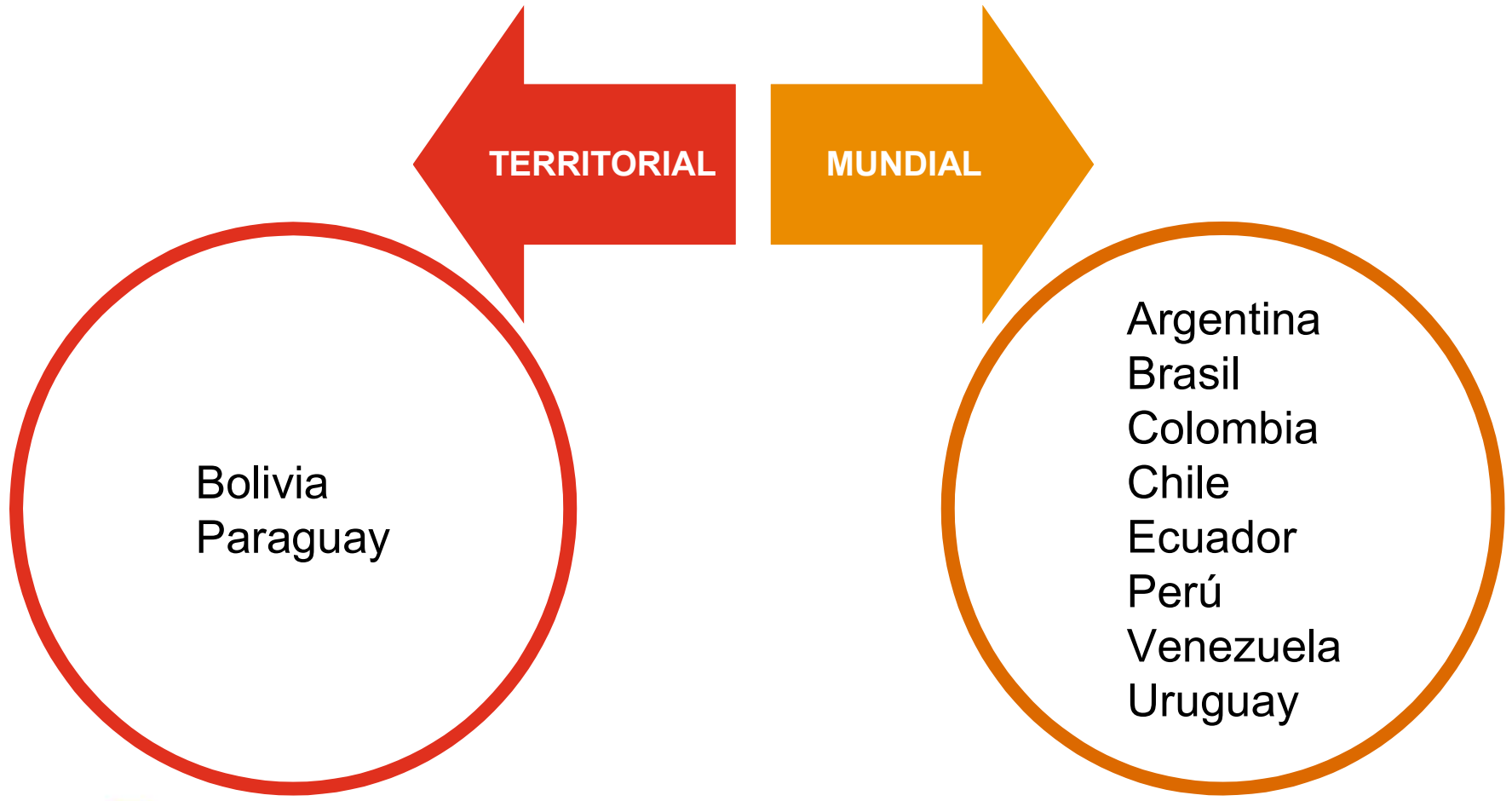
2

Sistemas de Imposición

Sistemas de Imposición



Sistemas de Imposición



3

Aspectos normativos
relevantes

Aspectos normativos relevantes

Art. 36° OBJETO

Se aplicará en todo el territorio nacional sobre las utilidades resultantes de los EEFF de las empresas al cierre de cada gestión anual, ajustadas.

Art. 37° 38° SUJETOS

Todas las empresas tanto públicas como privadas

Art. 49° EXENCIONES

- Actividades del Estado Nacional
- Instituciones no lucrativas
- Organismos internaciones de crédito e instituciones oficiales extranjeras
- Nueva industria en la ciudad de El Alto.

Aspectos normativos relevantes

**Art. 50
ALÍCUOTA**

Alícuota General 25%

**AA-IUE
Sector
Financiero**

25% cuando;

$\frac{\text{RAI}}{\text{Patrimonio neto}} > 6\%$

Aspectos normativos relevantes

**Art. 36°
BASE
IMPONIBLE**

Utilidad neta determinada de acuerdo con Principios de Contabilidad Generalmente Aceptados (PCGA) Ajustados con fines impositivos.

Utilidades

Rentas, beneficios o ganancias las que surjan de los estados financieros, tengan o no carácter periódico.

Aspectos normativos relevantes

Utilidad Neta Imponible

La que resulte de los EEFF de la empresa elaborados de conformidad con las normas de contabilidad generalmente aceptadas, con los ajustes y adecuaciones.

Exclusiones

Se excluirá de la base, las rentas de fuente extranjera y las rentas percibidas de otras empresas en carácter de distribución, siempre y cuando la empresa distribuidora de dichos ingresos sea sujeto pasivo de este impuesto

4

Principio de Fuente

Principio de Fuente

Principio de Fuente

- Bienes situados, colocados o utilizados económicamente en la República*.
- Cualquier acto o actividad susceptible de producir utilidades en el territorio nacional.
- Hechos ocurridos dentro del límite de la misma.



01

Remuneraciones percibidos por miembros de directorios, consejos u órganos directivos por actividades que efectúen en el exterior para empresas domiciliadas en Bolivia.

02

Alquileres y arrendamientos provenientes de inmuebles situados en el territorio de la República.

03

Intereses provenientes de depósitos bancarios efectuados en el país.

04

Actividades civiles, agropecuarias, mineras forestales, extractivas, comerciales e industriales o por la locación de obras o la prestación de servicios dentro del territorio de la República.

5

Cálculo del Impuesto

Cálculo del Impuesto



6

Ajustes Tributarios

Ajustes Tributarios – Gastos Deducibles

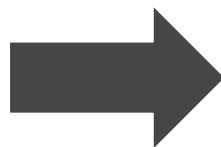
Regla General

Todos los gastos realizados tanto en el país como en el exterior, a condición de que estén **vinculados con la actividad gravada** y se encuentren respaldados con **documentos originales**.

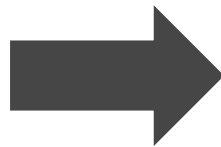
Gastos deducibles

Regla General

Todos los gastos realizados en el país y el exterior, a condición de:



- Estar vinculados con la actividad gravada.



- Estar respaldados con documentos originales.

Ajustes tributarios – Gastos No Deducibles

1

Gastos de viajes al interior y exterior del país, no sujetos a rendición de cuenta documentada ni debidamente respaldados con documentos originales, por el personal de la empresa.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" otorga a 2 de sus Dependientes y a 1 Consultor viáticos a cada uno por Bs 1.000 para la realización de un viaje a Cochabamba para asistir a una capacitación que tendrá la duración de 2 días, los viáticos cubren gastos de transporte, alimentación, y hospedaje. La rendición fue la siguiente:

El Dependiente N° 1 presentó su rendición incluyendo todas las facturas, recibos y respaldos en documentos originales y emitidas a su nombre.

El Dependiente N°2 presentó su rendición incluyendo todas las facturas, recibos y respaldos en fotocopias y emitidas a nombre de la empresa.

El Consultor presentó su rendición incluyendo todas las facturas, recibos y respaldos en fotocopias y emitidas a nombre de la empresa.



Ajustes tributarios – Gastos No Deducibles

2

- Donaciones efectuadas a entidades sin fines de lucro no reconocidas como exentas, que superen el 10% de la utilidad de esa gestión y no cumplan con los requisitos establecidos. (Contar con exención del beneficiario y no tener deudas tributarias)

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" sufre problemas de liquidez, y al no haber podido pagar los impuestos desde el mes de agosto; en el mes de diciembre realiza donaciones en efectivo a las siguientes 3 instituciones, con la finalidad de reducir el IUE de esa gestión que se determino en Bs10.000, de acuerdo al siguiente detalle:

1. Bs1.000 a una nueva ONG que se encuentra en proceso de constitución y elaboración de estatutos.
2. Bs 2.000 a una Institución sin fines de lucro que se dedica a la protección de animales y cuenta con la R.A. de exención formal.
3. Bs 500 a una Iglesia para la construcción de una nueva capilla, sin embargo el cura quien representa dicha institución podrá firmar el acta de recepción en el mes de junio debido a que se encuentra fuera de la ciudad hasta entonces.

Ajustes tributarios – Gastos No Deducibles

3

Pérdidas netas provenientes de operaciones ilícitas.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" sufrió el remolque con grúa de 2 de sus vehículos por encontrarse mal estacionados en una de las calles de la ciudad de La Paz. La multa por cada vehículo es de Bs600. Sin embargo, la empresa decidió sobornar a un funcionario público pagando Bs500 para que borre los registros del sistema con la finalidad de no pagar la multa establecida y la liberación inmediata de los vehículos.

Ajustes tributarios – Gastos No Deducibles

4

Gastos realizados, en el país y exterior, no vinculados con la actividad gravada ni respaldados con documentos originales

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" paga por concepto de mantenimiento y combustible de vehículos las facturas de acuerdo al siguiente detalle:

<i>Mantenimiento</i>	<i>Combustible</i>	<i>Detalle</i>
Bs100	Bs100	2 vehículos para uso en la Fabrica
Bs200	Bs200	1 vehículo para uso en las Oficinas centrales
Bs100	Bs100	3 vehículos para uso personal de Gerentes
Bs150	Bs150	9 vehículos para uso en Tiendas ubicadas en diferentes zonas de la ciudad

Ajustes tributarios – Gastos No Deducibles

5

Los retiros personales del dueño o socios ni los gastos personales de sustento del contribuyente y su familia.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa “ABC” decidió refaccionar su sala de reuniones, por lo que compro activos fijos con factura, de acuerdo al siguiente detalle:

<i>Activo Fijo</i>	<i>Importe</i>
1 Mesa	Bs10.000
10 Sillas	Bs6.000
4 Sillas ejecutivas	Bs6.000
1 Televisor	Bs4.000
1 Equipo de karaoke	Bs2.000
1 Data show portátil	Bs1.500
1 Mueble para TV	Bs3.000
1 Estante para libros	Bs1.500



Ajustes tributarios – Gastos No Deducibles

6

Remuneraciones a directores y síndicos que excedan la remuneración del principal ejecutivo asalariado de ese mes de la empresa.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" realizó el pago de remuneraciones en el presente mes, de acuerdo al siguiente detalle:

Gerente General	Bs10.000
Gerentes de área	Bs8.000
Jefes de área	Bs5.000
Asistentes	Bs3.000

Debido a que este mes los Directores y Síndicos se reunieron 2 veces por semana, para aprobar estatutos y tomar decisiones para la presentación de EEFF, la remuneración total a los mismos fue de Bs 10.000 a Directores y Bs5.000 a Síndicos.

Ajustes Tributarios - Ejemplos

La Empresa "ABC" realizó el pago de remuneraciones en el presente mes, de acuerdo al siguiente detalle:

Ejemplo

Gerente General	Bs10.000
Gerentes de área	Bs8.000
Jefes de área	Bs5.000
Asistentes	Bs3.000

Debido a que este mes los Directores y Síndicos se reunieron 2 veces por semana, para aprobar estatutos y tomar decisiones para la presentación de EEFF, la remuneración total a los mismos fue de Bs 10.000 a Directores y Bs5.000 a Síndicos.

GND: Bs5.000



Ajustes tributarios – Gastos No Deducibles

7

Gastos por servicios personales en los que no se haya retenido el RC-IVA correspondiente a los dependientes. Así como honorarios u otras retribuciones por asesoramiento, dirección o servicios prestados en el país o desde el exterior, demostrándose no haber retenido el impuesto correspondiente

8

IVA incorporado en el precio de compra de bienes y servicios que no resulta computable en la liquidación de dicho impuesto por estar asociado a operaciones no gravadas por el mismo.

Ajustes Tributarios - Ejemplos

Ejemplo

- Por la emergencia sanitaria, la compañía decide otorgar medicamentos de diferente tipo para evitar que las bajas médicas incrementen. Este importe no fue incluido en la planilla salarial debido a que se lo realiza solo una vez al año y no de forma habitual.
- Gastos por servicios de publicidad por Bs10.000 cuya factura llego a destiempo

Ajustes tributarios – Gastos No Deducibles

9

IUE, IT compensado con el IUE, ITF.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" muestra los siguientes saldos en su Estado de Resultados:

Impuesto a las Transacciones	Bs1.200
Impuesto a las Transacciones Financieras	Bs500
Impuesto a la propiedad de bienes inmuebles y vehículos automotores	Bs600
Tasas y patentes municipales	Bs200

(*) Se obtuvo utilidades en la gestión anterior por Bs10.000, por lo que se compensó todo el IT.

Ajustes tributarios – Gastos No Deducibles

10

Ajustes provenientes de transacciones no llevadas a precios de mercado.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa “ABC”, al momento de obtener el Estudio de Precios de Transferencia elaborado por sus consultores tributarios, evidenció una observación correspondiente a una desviación al no llevar a cabo transacciones a precios de mercado con sus empresas vinculadas del exterior, por concepto de servicios de asesoría legal, por lo que se muestra una desviación en los gastos incurridos de 5%, la cuenta de gasto “Asesoría legal del exterior” tiene un saldo de Bs1.000.

Ajustes tributarios – Gastos No Deducibles

11

Multas y accesorios (excepto intereses y MV) originados por la morosidad de tributos o en el incumplimiento de deberes formales.

Ajustes tributarios – Gastos no deducibles

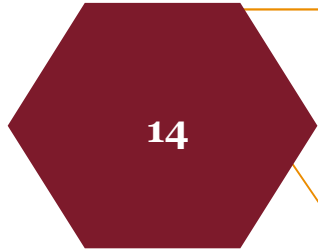
12

Aguinaldos y otras gratificaciones que se paguen al personal fuera de los plazos en que deba presentarse la DDJJ correspondiente a la gestión del año por el cual se paguen.

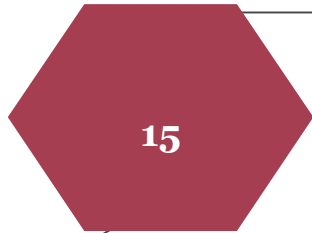
13

Previsiones o reservas de cualquier naturaleza, con excepción de los cargos anuales como contrapartida en la constitución de la previsión para indemnizaciones, incobrables y reservas técnicas.

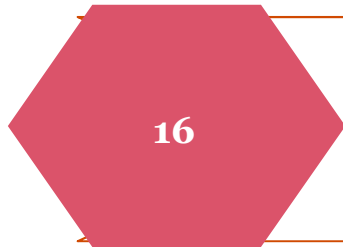
Ajustes tributarios – Gastos No Deducibles



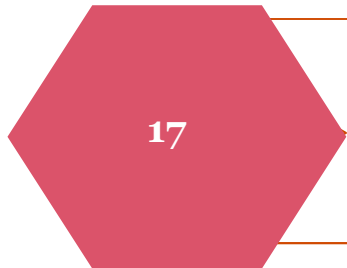
Reparaciones a Activos Fijos que superen el 20% del valor del bien.



Obsolescencia de activos y mercadería



Depreciaciones que pudieran corresponder a revalúos técnicos



Tasas de depreciación diferentes al DS.
Amortización derechos de llave, marcas de fabrica, etc. sin haber pagado un precio.

Ajustes tributarios – Gastos No Deducibles

18

Cuando en un año se obtenga una pérdida tributaria, ésta podrá deducirse de las utilidades gravadas obtenidas como máximo hasta los tres siguientes años.

Ajustes Tributarios - Ejemplos

La Empresa "ABC" obtuvo utilidad tributaria por Bs. 50.000. en la gestión 2020.

Ejemplo

Información Adicional:

Pérdida Tributaria 2016	Bs10.000
Pérdida Tributaria 2017	Bs7.000
Pérdida Tributaria 2018	Bs8.000
Pérdida Tributaria 2019	Bs2.000

Ajustes tributarios – Gastos no deducibles

19

Previsión para cuentas incobrables.

Ajustes Tributarios - Ejemplos

El primer año no se tiene incobrables

El segundo año ya contamos con un incobrable de Bs15.000.-

Entonces:

$$\begin{aligned} \text{Calculo incobrable} &= 150.000 * \frac{15.000}{120.000} \\ \text{Calculo incobrable} &= 18.750.- \end{aligned}$$

Ejemplo

Por tanto al 31-12-2015 se tendrá que constituir una previsión para incobrables por Bs18.750.-

Ajustes tributarios – Ingresos No Imponibles

20

Ingresos de fuente extranjera.

21

Rentas percibidas de otras empresas en carácter de distribución, siempre que la otra sea sujeta del IUE.

Ajustes Tributarios - Ejemplos

Ejemplo

La Empresa "ABC" presenta los siguientes ingresos:

- Ingreso por venta de bienes	Bs1.000
- Ingresos por intereses ganados inversiones locales	Bs500
- Ingresos por Intereses ganados inversiones exterior	Bs400
- Ingresos por dividendos en Coca Cola Bolivia	Bs300
- AITB	Bs200
- Diferencia de cambio	Bs100

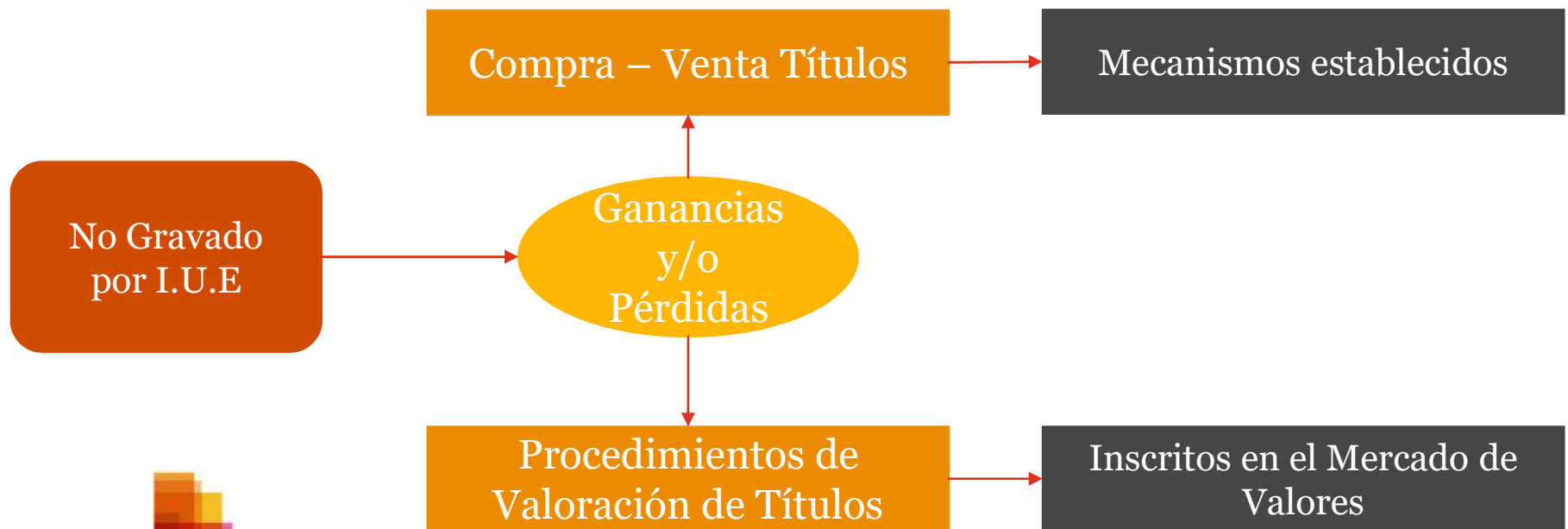
Disposiciones relacionadas al Mercado de Valores

LEY NRO. 1834
(Art. 117)

• Ley de Mercado de Valores (31-03-1998)

Ley Nro. 2064
(Art. 29)

• Ley de Reactivación Económica (03-04-2000)



Ajustes tributarios – Gastos No Deducibles propios de la Industria de Valores

1

Pérdida en compra - venta de valores registrados en el Mercado de Valores.

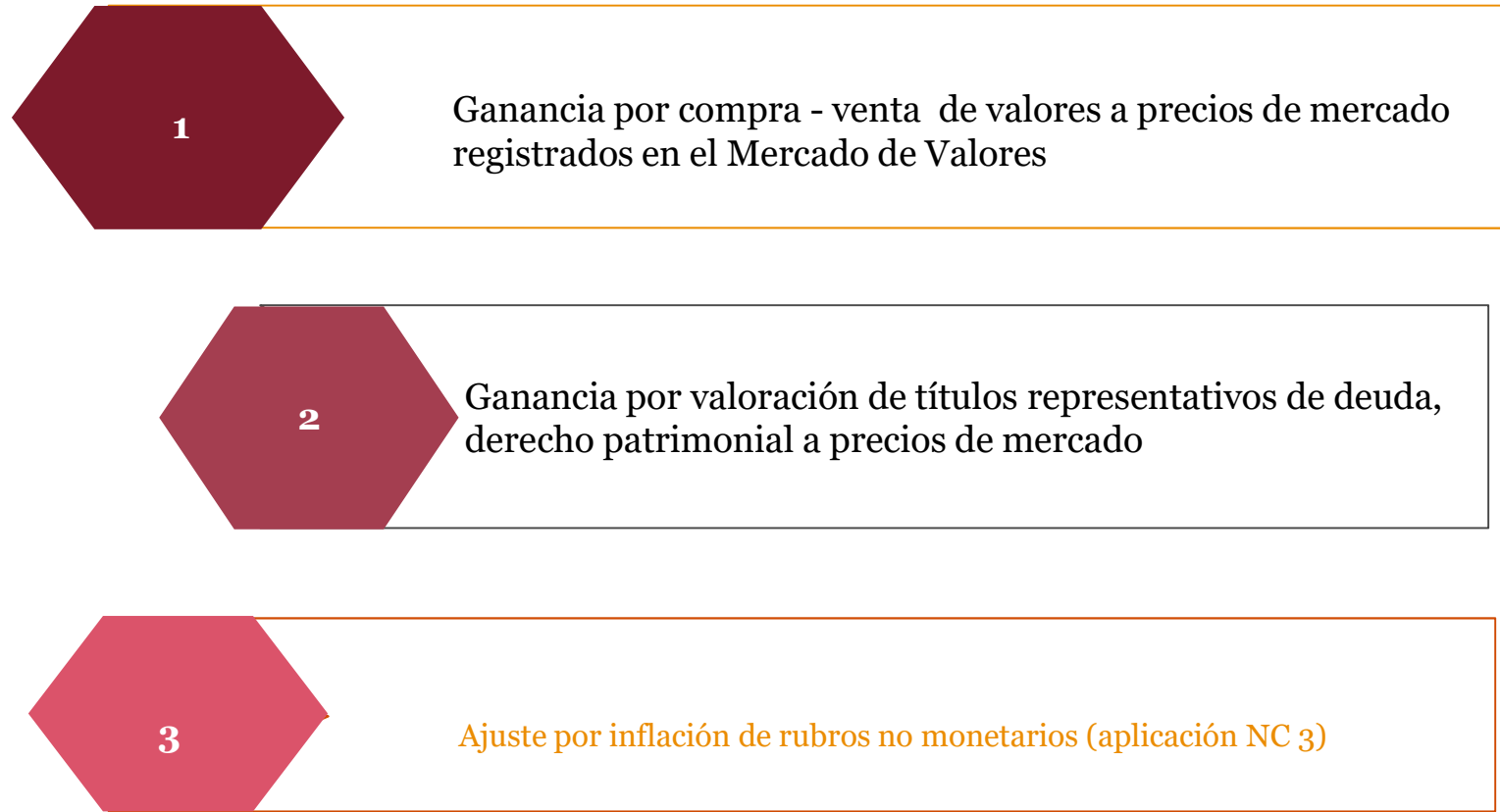
2

Pérdidas por valuación de títulos representativos de Deuda, Derecho Patrimonial

3

Ajuste originado por la Proporcionalidad de Gastos.

Ajustes tributarios – Ingresos No Imponibles propios de la Industria de Valores



Ajustes Tributarios - Proporcionalidad de Gastos

- Discriminar aquellos gastos directamente relacionados con ingresos gravados
- Discriminar aquellos gastos directamente relacionados con ingresos no gravados
- Aplicar la proporcionalidad a los gastos en los que no es posible realizar la discriminación con actividades gravadas y no gravadas

(*) La Normativa vigente no define un criterio específico para tal ajuste

Ajustes Tributarios - Proporcionalidad de Gastos

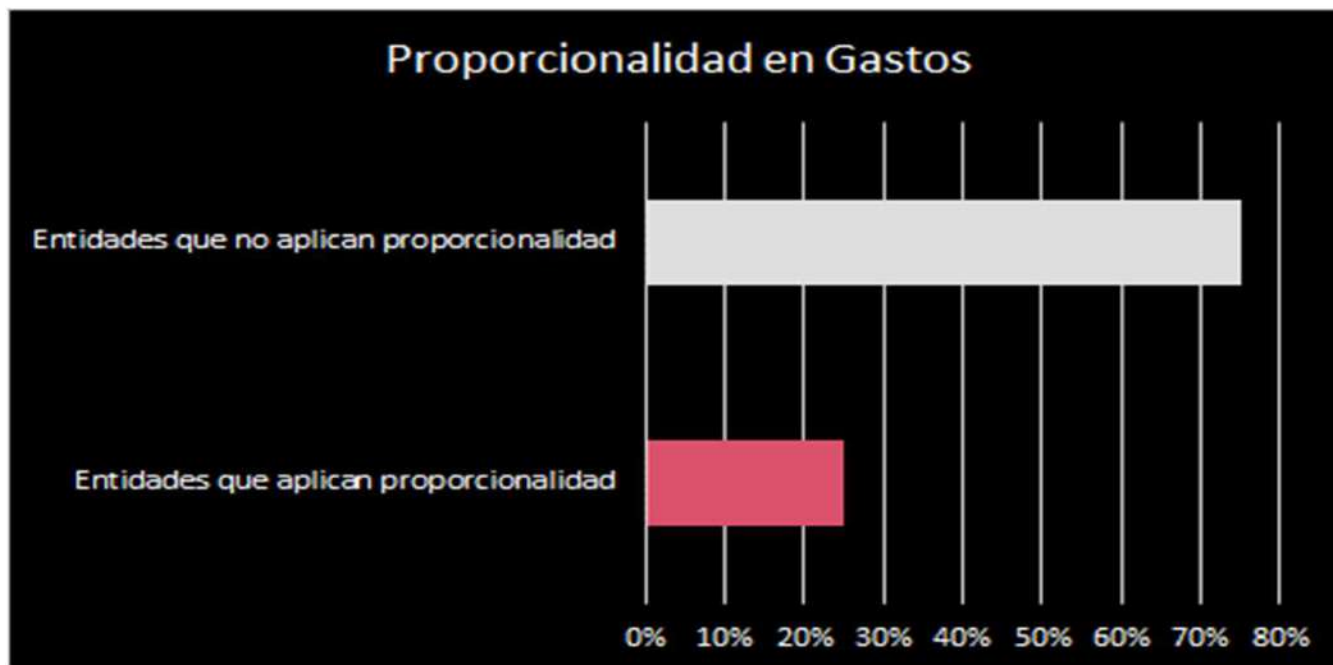
$$P.G. = \frac{I.N.I.}{T.I.} * G.S.C.P$$

Donde:

- P.G. : Proporcionalidad de Gastos
- I.N.I. : Ingresos no Imponibles o no Gravados
- T.I. : Total Ingresos
- G.S.C.P. : Gastos Sujetos a Criterios de Proporcionalidad



Ajustes Tributarios - Proporcionalidad de Gastos



DETALLE	PORCENTAJE
Entidades que aplican proporcionalidad	25%
Entidades que no aplican proporcionalidad	75%
Total	100%

8

Prórrogas Tributarias

Prórroga I.U.E. – Contribuyentes Resto

*D.S. Nro.
4249*

- Se prorroga la declaración, determinación y pago del cien por ciento (100%) del Impuesto sobre las Utilidades de las Empresas hasta el 31 de Julio de 2020 para todos aquellos contribuyentes pertenecientes al Régimen General Categoría Resto de Contribuyentes.

*Prórroga
Escalonada*

01

50% del I.U.E. hasta el 31 de Julio de 2020 (Prorroga excepcional de Oficio)

02

15% del I.U.E. hasta el 31 de Agosto de 2020 (Sin Mantenimiento de valor, intereses y sanciones)

03

15% del I.U.E. hasta el 30 de Septiembre de 2020 (Sin Mantenimiento de valor, intereses y sanciones)

04

20% del I.U.E. hasta el 30 de Octubre de 2020 (Sin Mantenimiento de valor, intereses y sanciones)



(*)Si el I.U.E ya se canceló al 31 de Mayo de 2020, **se puede realizar una rectificación en favor del Fisco** hasta el 31 de Julio de 2020 y pagar el saldo incrementado sin mantenimiento de valor, intereses y sanciones.

Prórrogas Tributarias

OBLIGACIÓN TRIBUTARIA	PERIODO FISCAL	PRÓRROGA DE VENCIMIENTO
<ul style="list-style-type: none">• Declaración y pago de obligaciones tributarias mensuales• Obligaciones Formales (LCV, Agentes de Información y otros)• Cuotas Facilidades de Pago• Presentación Física y Digital de Estados Financieros, Memoria Annual, Información Tributaria Complementaria y Precios de Transferencia	<ul style="list-style-type: none">• Febrero, Marzo, Abril y Mayo 2020• Febrero, Marzo, Abril y Mayo 2020• Octubre 2019/Junio 2020• Contribuyentes con Cierre al 31 de Diciembre 2019	<ul style="list-style-type: none">• Hasta el vencimiento del Periodo fiscal de Junio 2020 según ultimo digito de NIT• Hasta el vencimiento del Periodo fiscal de Junio 2020 según ultimo digito de NIT• Hasta el 31 de Julio de 2020• Hasta Julio según último dígito de NIT

Prórrogas Tributarias

OBLIGACIÓN TRIBUTARIA	PERIODO FISCAL	PRÓRROGA DE VENCIMIENTO
<ul style="list-style-type: none">• Formulario 110 Dependientes• Envío Planilla Tributaria• Presentación de Solicitudes de Devolución Impositiva (CEDEIMs)• Presentación de Solicitudes de Certificados de Notas de Credito Fiscal (CENOCREFs)	<ul style="list-style-type: none">• Abril y Mayo 2020• Abril, Mayo y Junio 2020• Periodos Fiscales Septiembre a Diciembre 2019 con vencimiento de Marzo a Junio 2020• Periodos Fiscales Septiembre a Diciembre 2019 con vencimiento de Marzo a Junio 2020	<ul style="list-style-type: none">• Hasta el 20 de Junio 2020• Hasta el vencimiento del Periodo fiscal de Junio 2020 según ultimo digito de NIT• Hasta el 31 de Julio de 2020• Hasta el 30 de Julio de 2020

9

Ejercicio Práctico

Ejercicio Práctico

Ejercicio

Usted debe determinar el IUE, en el marco de la Ley Nro 843 y el Decreto Supremo Nro 24051. La sociedad del ejemplo expondrá su información corresponde a la gestión 2020 (enero a diciembre).

- 1.- Las sociedad percibió comisiones por intermediación bursátil por Bs 2.000.000.-
- 2.- La Sociedad percibió comisiones por servicios de valoración de cartera por Bs100.000
- 3.- La Sociedad percibió ganancias por venta e valores bursátiles por Bs 3.000.000.
- 4.- La Sociedad generó rendimientos por inversión bursátiles por Bs 1.500.000
- 5.- La Sociedad tiene gastos por servicios de intermediación por Bs 500.000



Ejercicio Práctico

Ejercicio

6.- La Sociedad tiene gastos por administración y custodia 400.000

7.- La Sociedad tiene pérdida en venta de valores bursátiles por Bs 1.500.000

8.- La Sociedad registra gastos por personal por Bs 1.000.000 de los cuales se tienen pagos por bonos Bs 400.000 los cuales no ingresaron a la planilla tributarias.

9.- La Sociedad registra gastos de comercialización por Bs 60.000

10.- La Sociedad registra por impuestos Bs 350.000 de los cuales Bs30.000 corresponde a la provisión para impuestos municipales y Bs 10.000 por ITF

Ejercicio Práctico

Ejercicio

- 11.- La Sociedad registra gastos por administración por Bs 800.000 de los cuales Bs50.000 corresponde a una cena navideña para el personal
- 12.- La Sociedad registra por depreciación Bs 200.000
- 13.- La Sociedad registra por servicios contratados Bs100.000
- 14.- La gestión anterior la Sociedad obtuvo una pérdida tributaria de Bs500.000.
- 15.- El ajuste por inflación neto alcanzó a Bs120.000 (gasto).

Gracias

[pwc.com](https://www.pwc.com)

© 2020 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

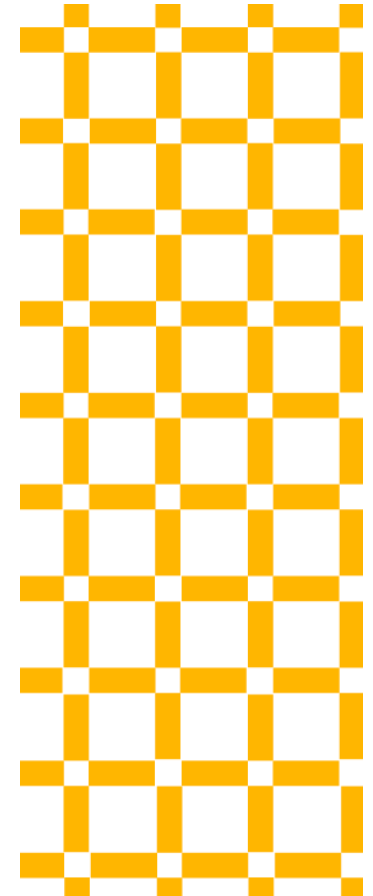
Implementación de Normas Internacionales de Auditoría y Normas Internacionales para el Ejercicio de la Práctica de Auditoría Interna

Programa de Capacitación - ABAV
Julio, 2020



Contenido

1. Antecedentes y marco normativo
2. Preparación de papeles de trabajo
3. Preparación y presentación de informes, roles, responsabilidades y funciones del auditor interno



1

Antecedentes y marco normativo

1.1 Antecedentes

Definición de auditoría interna

ASFI Valores (RNMV, Libro 11. Título II, Capítulo 1, Sección 1, Art 3)

Auditoría interna es la actividad **independiente y objetiva** de control eficiente, aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una entidad supervisada, aportando un enfoque sistemático y disciplinado, contribuyendo así al logro de los objetivos de la entidad supervisada.



Instituto de auditores internos (IAI)

Auditoría interna es una actividad **independiente y objetiva** de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno.

1.2 Marco normativo

De acuerdo con el inciso b, artículo 1, Sección 5, Capítulo I, Título II del Libro 11 de la RNMV de ASFI, la unidad de auditoría interna debe desempeñar su trabajo conforme:

01

Normas de auditoría generalmente aceptadas en Bolivia (NAGA) emitidas por el CTNAC

02

Normas internacionales de auditoría (NIA) emitidas por el IAASB (por sus siglas en inglés)

03

Código Internacional de Ética para Profesionales de la Contabilidad del IESBA

1.2 Marco normativo



El Instituto de Auditores Internos (IAI) es una organización reconocida internacionalmente que establece estándares para la práctica de la profesión de auditoría interna.

Es común que, las funciones de auditoría interna establezcan su metodología, políticas y prácticas en conformidad con los estándares del IAI.



Importante recordar!

NAGA's están formadas por (Resolución CTNAC/01/2015):

- La NA 1 "Normas básicas de auditoría de estados financieros" emitidas por el CTNAC.
- Las NIA emitidas por el IAASB.

1.2 Marco normativo

El auditor interno debe desempeñar su trabajo:



El auditor interno puede alinear sus metodologías, políticas y prácticas:



1.3. Principales normas relacionadas con la preparación de papeles de trabajo

NAGA's (incluye NIA's)

- NA N° 1: Normas básicas para una auditoría de estados financieros
- NIA 230: Documentación de auditoría
- NIA 240: Responsabilidades del auditor relacionadas a fraude en una auditoría de estados financieros
- NIA 315: Identificación y evaluación de error de riesgo material
- NIA 330: Respuestas de auditoría a la evaluación de riesgos
- NIA 500: Evidencia de auditoría
- NIA 501: Evidencia de auditoría: Consideraciones específicas para partidas seleccionadas

NIEPAI's

- Norma sobre desempeño 2210: Objetivos del trabajo
- Norma sobre desempeño 2220: Alcance del trabajo
- Norma sobre desempeño 2240: Programa de trabajo
- Norma sobre desempeño 2310: Identificación de la información
- Norma sobre desempeño 2320: Análisis y evaluación
- Norma sobre desempeño 2330: Documentación de la información

1.3. Principales normas relacionadas con la preparación de papeles de trabajo

NAGA's (incluye NIA's)

- NIA 505: Confirmaciones externas
- NIA 520: Procedimientos analíticos
- NIA 530: Muestreo de auditoría
- NIA 540: Auditoría de estimaciones contables
- NIA 550: Partes relacionadas
- NIA 560: Eventos subsecuentes
- NIA 570: Empresa en marcha

NIEPAI's

- Norma sobre desempeño 2340: Supervisión del trabajo

1.4 Principales normas relacionadas con la preparación de informes

NAGA's (incluye NIA's)

- NIA 700: Formación de la opinión y emisión del informe de auditoría
- NIA 701: Comunicación de las cuestiones clave de auditoría
- NIA 705: Modificaciones en la opinión del auditor independiente
- NIA 706: Párrafos de énfasis y de otras cuestiones en el informe del auditor
- NIA 720: Responsabilidad del auditor respecto a otra información
- NIA 800: Consideraciones especiales – Auditoría de estados financieros preparados de acuerdo con un marco de propósito específico

NIEPAI's

- Norma sobre desempeño 2400: Comunicación de resultados
- Norma sobre desempeño 2410: Criterios para la comunicación
- Norma sobre desempeño 2420: Calidad de la comunicación
- Norma sobre desempeño: 2421 Errores u omisiones
- Norma sobre desempeño 2430: Uso de “Realizado de conformidad con Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna”
- Norma sobre desempeño 2431: Declaración de incumplimiento de normas

1.4 Principales normas relacionadas con la preparación de informes

NAGA's (incluye NIA's)

- NIA 805: Consideraciones especiales – Auditoría de un solo estado financiero o de un elemento, o partida de un estado financiero
- NIA 810: Encargos para informar sobre estados financieros resumidos
- NIER 2400: Encargos de revisión de estados financieros
- NIER 2410: Revisión de información financiera Intermedia
- NISR 4400: Encargos de procedimientos Previamente acordados
- NISR 4410: Encargos de compilación
- NIEA 3000: Encargos de aseguramiento distintos de la auditoría o de la revisión de la información financiera histórica

NIEPAI's

- Norma sobre desempeño 2450: Opiniones globales
- Norma sobre desempeño 2440: Difusión de resultados
- Norma sobre desempeño 2500: Seguimiento del proceso
- Norma sobre desempeño 2600: Comunicación de la aceptación de los riesgos

2

Preparación de papeles de trabajo

2.1 Importancia de la documentación de auditoría

Por qué es importante la documentación de auditoría en los papeles de trabajo?

Why is audit documentation important?



Context

2.1 Importancia de la documentación de auditoría

Por qué es importante la documentación de auditoría en los papeles de trabajo?

Soporta las conclusiones y la opinión de auditoría

Refleja en detalle el trabajo realizado por el auditor

Permite alcanzar las mismas conclusiones del auditor, a través de la revisión objetiva de un tercero

Permite cumplir con los estándares de calidad en industrias reguladas

Demuestra el trabajo realizado por el auditor durante todo el proceso

Documentación de auditoría de acuerdo con NAGA (incluye NIA)

2.2 Objetivo de los papeles de trabajo (NA)

NA 1 – Evidencia de auditoría

El auditor debe obtener evidencia de auditoría suficiente y competente a través de la aplicación de:

- i) procedimientos de cumplimiento, y*
- ii) procedimientos sustantivos,*

para obtener conclusiones razonables en las cuales base su opinión sobre la información financiera.

2.2 Objetivo de los papeles de trabajo (NIA)

NIA 230.5 – Objetivo

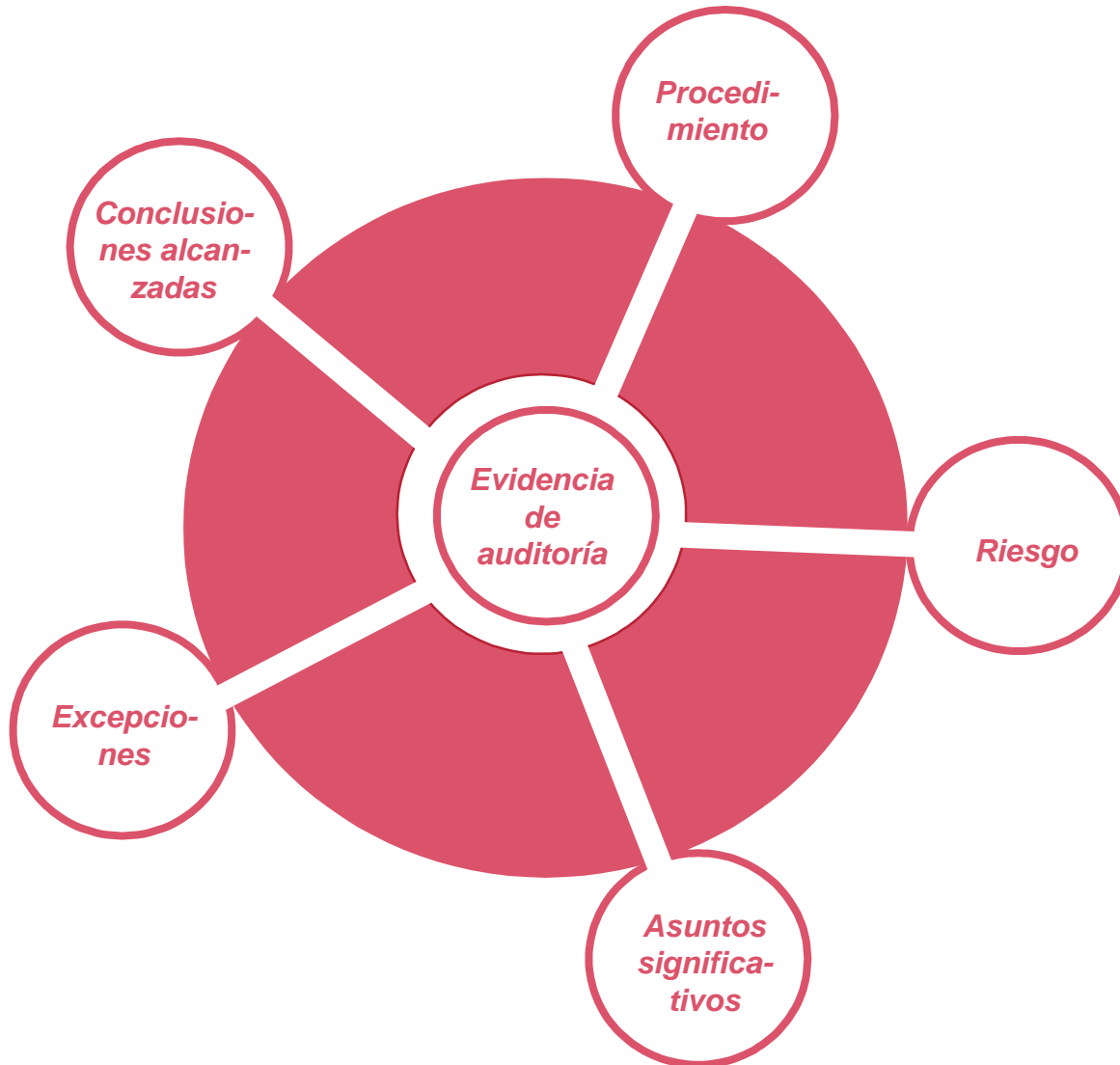
El objetivo del auditor es preparar la documentación de auditoría que brinde:

Un registro suficiente y apropiado de la base para el informe del auditor; y

Evidencia de que la auditoría se planificó y llevó a cabo de acuerdo con las NIA y requerimientos aplicables legales y regulatorios.

2.2 Objetivo de los papeles de trabajo (NIA)

Cómo documentamos evidencia suficiente y apropiada?



2.3 Forma, contenido y alcance de la documentación de auditoría

NIA 230

NIA 230.8. El auditor deberá preparar la documentación de auditoría para permitir que un auditor experimentado, que no tiene conexión previa con la auditoría, comprenda:

La naturaleza, oportunidad y alcance de los procedimientos realizados para cumplir con las NIA y los requisitos legales y regulatorios aplicables;

1

Los resultados de los procedimientos de auditoría y la evidencia de auditoría obtenida; y

2

Asuntos significativos que surjan durante la auditoría y las conclusiones arribadas, y las opiniones profesionales significativas hechas al alcanzar esas conclusiones.

3

2.3 Forma, contenido y alcance de la documentación de auditoría

NIA 230



Forma, contenido y alcance

- Tamaño, complejidad entidad
- Naturaleza de los procedimientos
- Riesgos de error material
- Nivel de la evidencia obtenida



Documentación a incluir:

- Programas de auditoría
- Análisis efectuado
- Memo de asuntos relevantes
- Resumen de asuntos significativos
- Conclusiones



2.4 Documentación de asuntos significativos y juicios profesionales relacionados

NIA 230

Asuntos que dan lugar a asuntos significativos (NIA 315)

Dificultades para aplicar procedimientos de auditoría (Limitaciones)

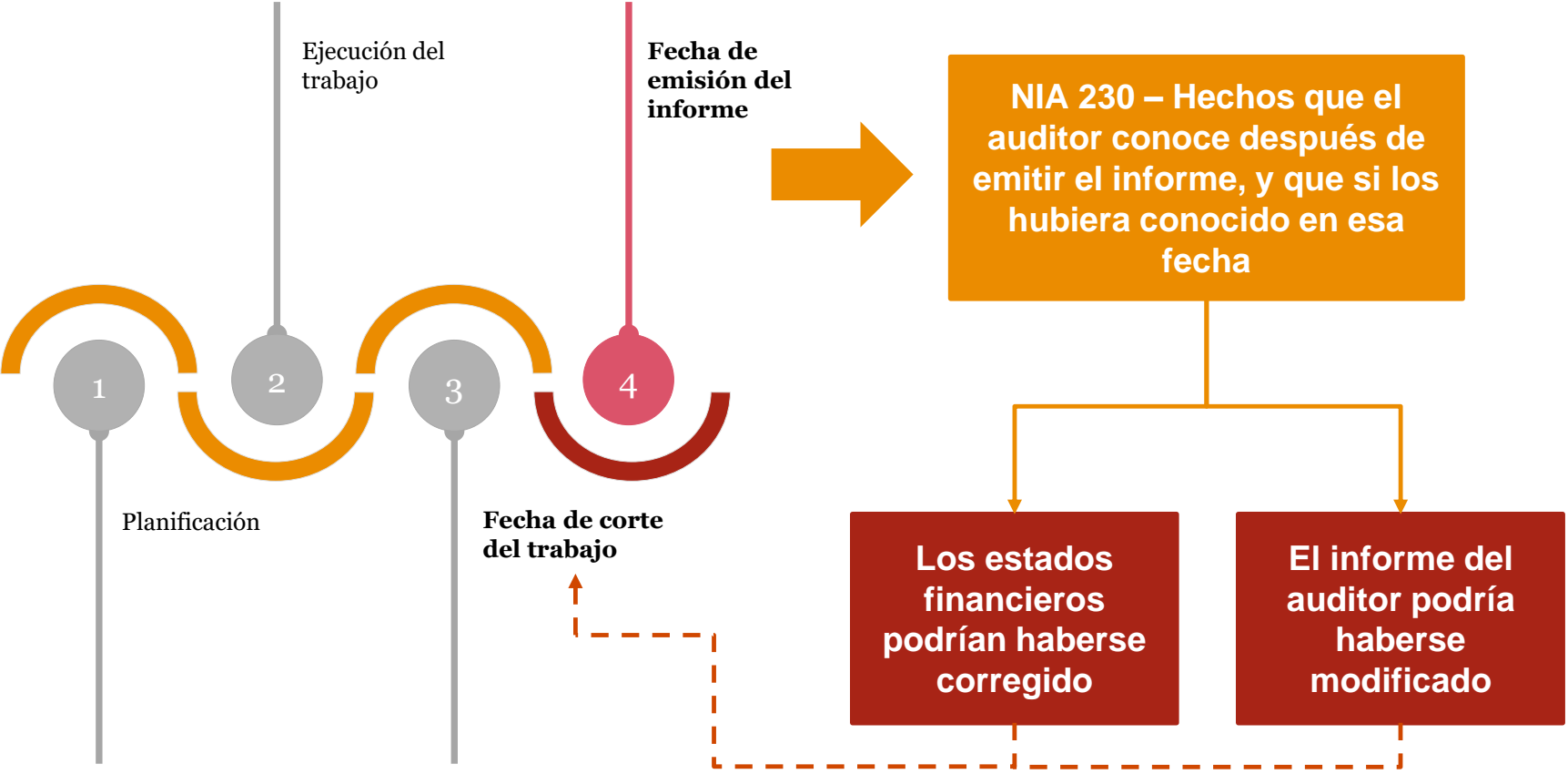
Resultados de los procedimientos de auditoría (errores materiales, reevaluar riesgos y respuestas)

Discusiones con la Gerencia, Gobierno corporativo de los asuntos significativos

Hallazgos que podrían resultar en la modificación de la opinión de la auditoría

2.5 Documentación de asuntos que surgen después de la fecha del informe del auditor

NIA 230



2.6 Ensamblaje del archivo del file de auditoría

NIA 230

ISQC 1. Los auditores/firmas deben establecer políticas y procedimientos para la finalización oportuna del ensamblaje de los archivos de auditoría.



Oportuno = No más de 60 días !

NIA 230. A22. El ensamblaje es un proceso administrativo que no implica la realización de nuevos procedimientos de auditoría o la extracción de nuevas conclusiones.

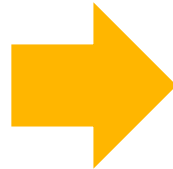
2.6 Ensamblaje del archivo del file de auditoría

NIA 230

El proceso administrativo principalmente es:

- Reemplazar documentos originales por copias.
- Incluir referencias finales a los papeles.
- Incluir lista del archivo de ensamblaje.
- Otros.

Retención de documentación



No inferior a 5 años a partir de la fecha de emisión del informe

2.7 Documentación de las responsabilidades del auditor en relación con el riesgo de fraude

NIA 240

01

Las decisiones importantes alcanzadas durante la discusión entre el equipo del compromiso con respecto a la susceptibilidad de los estados financieros de la entidad a errores materiales debido a fraude

02

Los riesgos de error material debido a fraude a nivel de estado financiero y asección; la naturaleza, oportunidad y alcance de los procedimientos, y sus respuestas de auditoría.

03

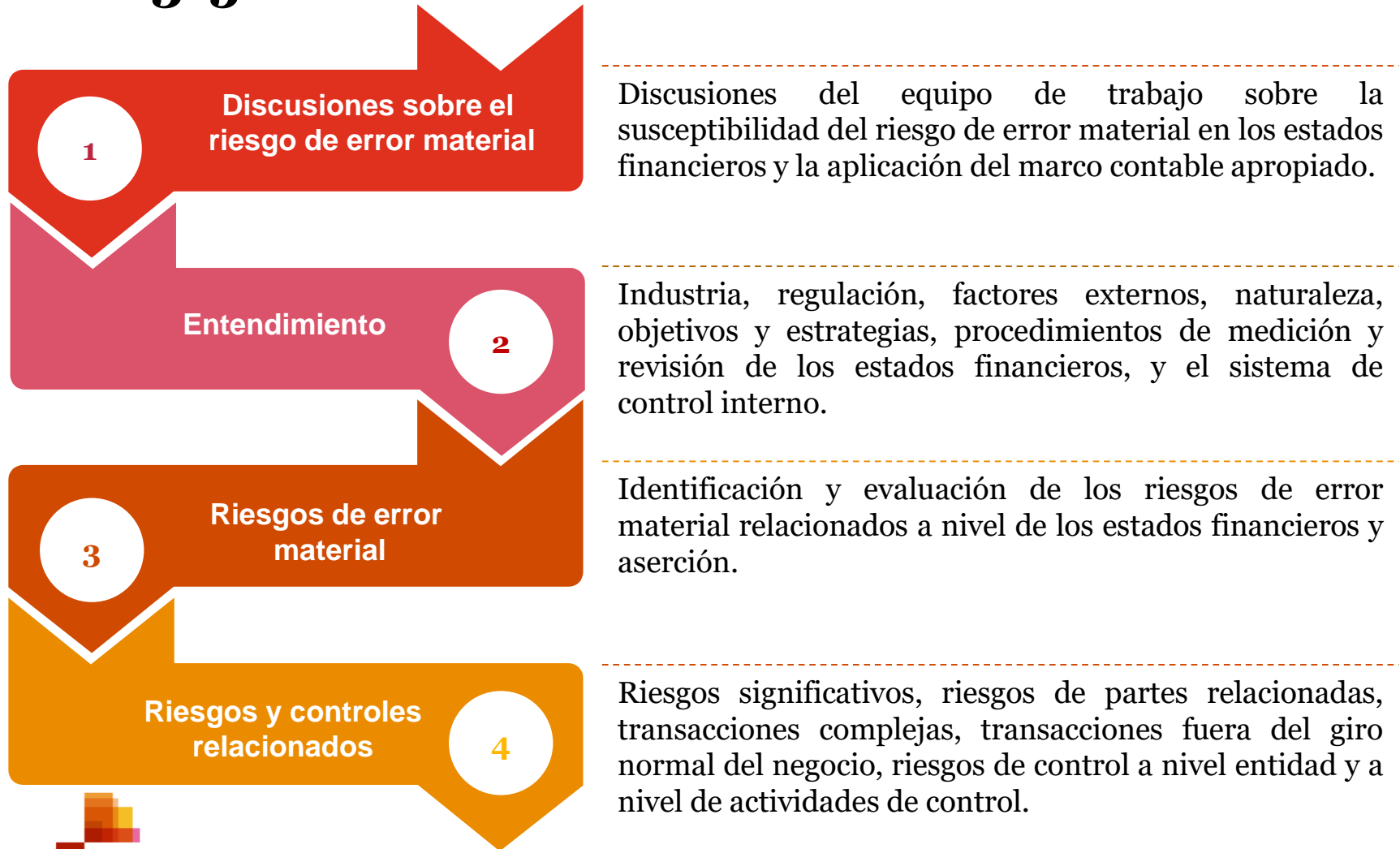
Las respuestas y resultados de los procedimientos de auditoría para abordar el riesgo de la “vulneración de controles por parte de la gerencia”.

04

La documentación de las razones cuando el riesgo de “reconocimiento de ingresos” no es aplicado o refutado para el compromiso.

2.8 Documentación de la identificación y evaluación del riesgo de error material

NIA 315



2.9 Documentación de las respuestas a los riesgos evaluados

NIA 330

Respuestas generales para abordar los riesgos de error material, la naturaleza, oportunidad y alcance de dichos procedimientos

01

Si se utiliza la evidencia sobre la efectividad de controles de auditorías anteriores, deberá documentarse las conclusiones

02

Reconciliación de los estados financieros y los registros contables (journal entries)

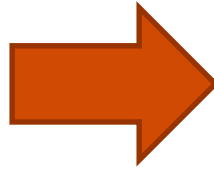
03

Documentación de asuntos significativos

Documentación de asuntos significativos

Qué son?

Hallazgos o asunto que a juicio del auditor es significativo



Tienen directa relación con la opinión o con el soporte de la misma

Ejemplos:

- Diferencias materiales sobre los estados financieros o sobre una cuenta,
- Riesgos que fueron identificados durante la planificación de la auditoría,
- Limitaciones al trabajo del auditor,
- Impacto de COVID-19.

Requieren consultas

Documentación de asuntos significativos

Qué debemos documentar?

- Descripción del asunto, antecedentes y circunstancias.
- Evidencia de auditoría obtenida y evaluada.
- Información inconsistente.
- Consultas requeridas.
- Registro de las discusiones.
- Conclusiones.

Ejemplo

De acuerdo con la auditoría programada de la cuenta “provisiones” al 30 de junio de 2019, se ha solicitado los estados de cuenta de provisiones a la fecha de corte. En el estado de cuenta se identifica un proveedor que representa el 10% del saldo y el restante 90% solo se incluye en una línea de “otros proveedores”. El auditor interno definió realizar procedimientos de auditoría para verificar el saldo de la cuenta para la auditoría programada. Los resultados de la auditoría fueron discutidos con la Gerencia de Finanzas el 14/09/2019, quien confirmó los resultados obtenidos por el auditor y que serán incluidos en la opinión.

Documentación de asuntos significativos

Descripción del asunto, antecedentes y circunstancias

De acuerdo con la auditoría programada de la cuenta provisiones al 30 de junio de 2019, se ha solicitado los estados de cuenta de provisiones a la fecha de corte. Revisado el estado de cuenta se identificaron partidas por un monto de Bs1 millón (90% del saldo) que no cuentan con documentación de soporte.

Evidencia de auditoría obtenida

Se realizaron los siguientes procedimientos para verificar el saldo de la cuenta conforma a NCGA:

- Cotejamos el estado de cuenta con los saldos de la cuenta a la fecha de corte.
- Efectuamos confirmaciones de saldos a una muestra de proveedores para corroborar los saldos. Para las respuestas enviadas, efectuamos procedimientos alternativos.
- Verificamos los registros contables de gastos con la documentación soporte respectiva.

Como resultado de los procedimientos se ha identificado: i) El estado de cuenta identifica un proveedor que representa el 10% del saldo, y el restante 90% no tiene identificado a los proveedores, ii) no obtuvimos respuesta del cliente confirmado, pero se verificó el saldo a través del pago posterior, iii) sobre el 90% del saldo de provisiones, seleccionamos una muestra significativa para verificar la documentación de respaldo de origen o el pago posterior, sin embargo no nos fue entregada documentación alguna.

Documentación de asuntos significativos

Información inconsistente

No se ha identificado información inconsistente o que contradiga los resultados obtenidos.

Consultas requeridas

El auditor encargado, consultó con el Director de la Unidad de Auditoría y se confirmaron las mismas conclusiones. En este sentido se sugirió incluir el siguiente párrafo de salvedad por limitación al alcance en el informe de auditoría.

“Al 30 de junio de 2019, la Sociedad debitó la cuenta “gastos varios” y acreditó la cuenta “provisiones” por Bs1.000.000. No nos ha sido posible obtener información suficiente que sustente dicha contabilización ni nos ha sido posible satisfacernos en cuanto al valor en libros de las cuentas antes mencionadas por otros procedimientos de auditoría.”

Documentación de asuntos significativos

Registro de discusiones

En fecha 14 de septiembre de 2019, se ha discutido con el Gerente Financiero Sr. Juan Perez sobre los resultados de la auditoría programada de la cuenta de “provisiones” detallados en **Evidencia de auditoría obtenida**. Al respecto la Gerencia Financiera confirmó los resultados obtenidos por el auditor y aceptó que serán incluidos en la opinión.

Conclusiones

El Director de la UAI con el equipo asignado para el trabajo, definieron incluir el siguiente párrafo en el informe de la auditoría programada.

“Al 30 de junio de 2019, la Sociedad debitó la cuenta “gastos varios” y acreditó la cuenta “provisiones” por Bs1.000.000. No nos ha sido posible obtener información suficiente que sustente dicha contabilización ni nos ha sido posible satisfacernos en cuanto al valor en libros de las cuentas antes mencionadas por otros procedimientos de auditoría.”

Asimismo se incluirán el informe y resultados en el siguiente comité de auditoría.

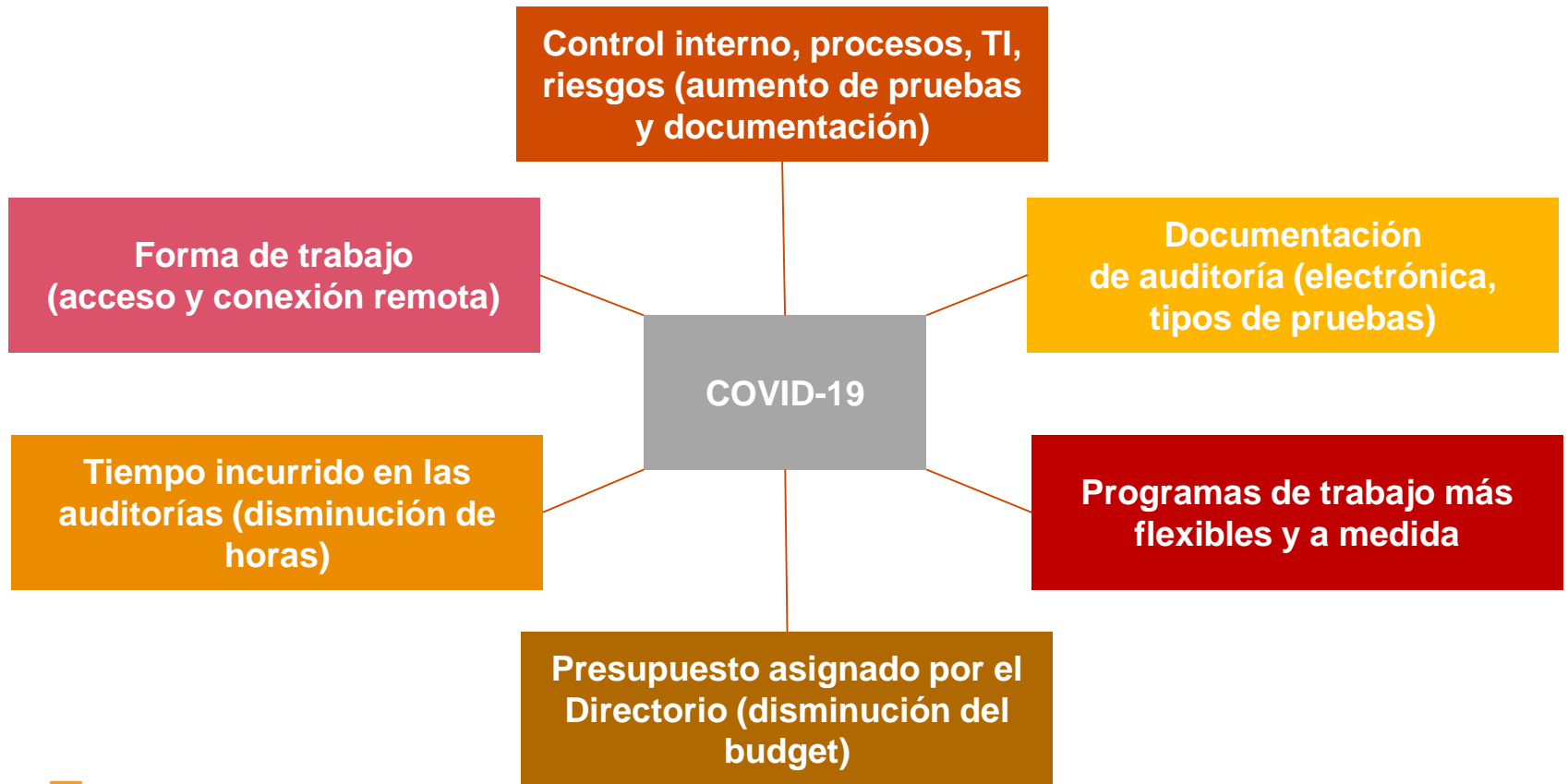
Documentación de asuntos significativos

Principales impactos de COVID-19 a nivel de negocio



Documentación de asuntos significativos

Principales impactos de COVID-19 en la función de auditoría interna



Documentación de asuntos significativos

Principales aspectos a considerar en la evaluación de COVID-19

Con carácter enunciativo y no limitativo, los principales aspectos a considerar en la evaluación del sistema de control interno y en los riesgos del negocio, entre otros, podrían ser:

- ✓ Según fuera aplicable, que se reevalúen los riesgos en los controles operativos originados por las actualizaciones/modificaciones de los procedimientos internos para que el personal actualmente trabaje remotamente en los procesos clave del negocio (ej: oficiales de inversión, administración de fondos, inversiones, entre otros).
- ✓ Según fuera aplicable, si se adecúan los procedimientos de control interno en los procesos operativos, que se asegure que dichos cambios no originarían una posible disminución de los controles de monitoreo/supervisión, incompatibilidad en segregación de funciones, mayores accesos o privilegios o niveles autorización no permitidos en los sistemas, entre otros.
- ✓ Según fuera aplicable, que se reevalúen los riesgos de los controles generales de tecnologías de información (TI) por un posible aumento en la habilitación de accesos al personal a través de canales remotos.

Documentación de asuntos significativos

Principales aspectos a considerar en la evaluación de COVID-19

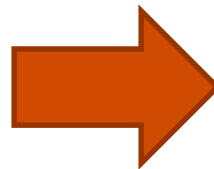
- ✓ Según fuera aplicable, que se reevalúen los riesgos de fraude que podrían estar relacionados a los procedimientos aplicados en el trabajo remoto.
- ✓ Según fuera aplicable, que se reevalúe si en el ambiente de tecnologías de la información (TI) se hubiera originado un incremento en el riesgo de ciberseguridad por el aumento de accesos a través de canales remotos.
- ✓ Según fuera aplicable, que se identifiquen las áreas, procesos y formas de archivo/custodia de la documentación electrónica que quedaría archivada producto de posibles cambios que se hayan realizado en los procesos operativos.
- ✓ Según fuera aplicable, que se actualicen las proyecciones en el presupuesto y otros aspectos relevantes en el plan estratégico (ej: objetivos, estrategias, entre otros) tomando en cuenta el contexto económico y condiciones actuales.
- ✓ Según fuera aplicable, que se reevalúen los criterios aplicados en el proceso de evaluación integral de riesgos, para analizar posibles actualizaciones/adecuaciones en los procedimientos, escenarios o supuestos (liquidez, mercado, crediticio, entre otros)

Documentación de las respuestas a los riesgos evaluados

Documentación de las respuestas a los riesgos evaluados

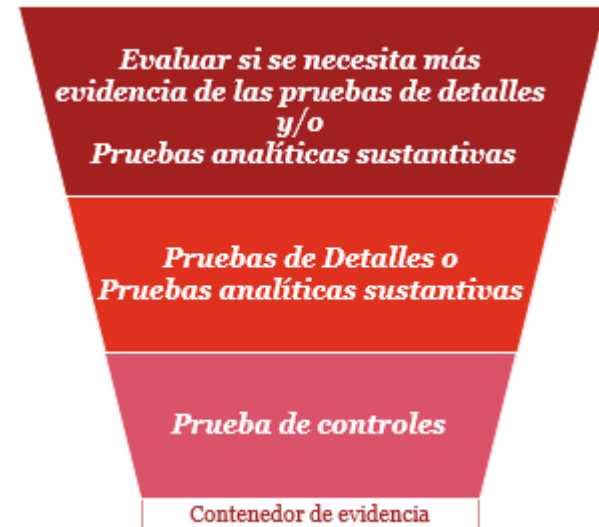
Razones cuando el riesgo de “reconocimiento de ingresos” no es aplicado o refutado

El reconocimiento de ingresos es un riesgo significativo



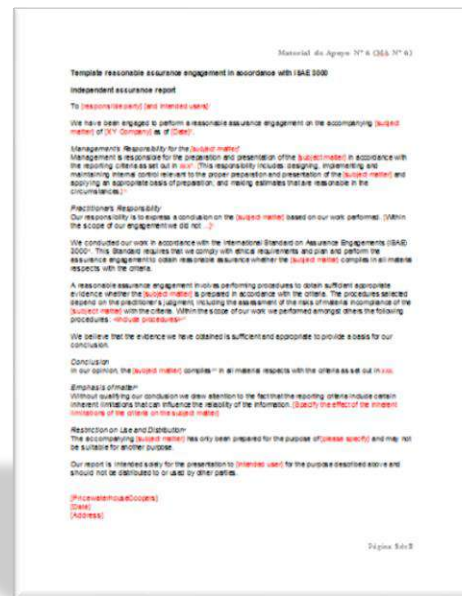
Tiene impacto directo en la naturaleza, alcance y oportunidad de los procedimientos de auditoría

La definición del riesgo de “revenue recognition” impactará en el nivel de evidencia requerida



Documentación de las respuestas a los riesgos evaluados

Ejemplo – Refutación del riesgo de Revenue recognition (Caso Banco ABC)



Documentación de auditoría de acuerdo con NEPAI

2.10 Objetivo de los papeles de trabajo (NIEPAI)

NIEPAI 2330 – Documentación de la información

Los auditores internos deben documentar información suficiente, fiable, relevante, y útil que les permita respaldar los resultados del trabajo y las conclusiones.

Se debe controlar el acceso a los registros del trabajo y se debe obtener la aprobación de la alta administración o asesores para otorgar acceso a terceros.

Se debe establecer políticas sobre la custodia y retención de los registros de trabajos de consultoría y sobre la posibilidad de darlos a conocer a terceros.

2.11 Propósito, supervisión y control, y documentación y archivo de los papeles de trabajo (PT)

NIEPAI 2330

Propósito

- Ayudan en la planificación, ejecución y revisión de trabajos.
- Es el soporte principal de los resultados del trabajo.
- Confirma si los objetivos se han alcanzado.
- Soporta la precisión e integridad del trabajo realizado.
- Define el programa de procedimientos de aseguramiento.
- Facilita la revisión de terceras partes.

Supervisión

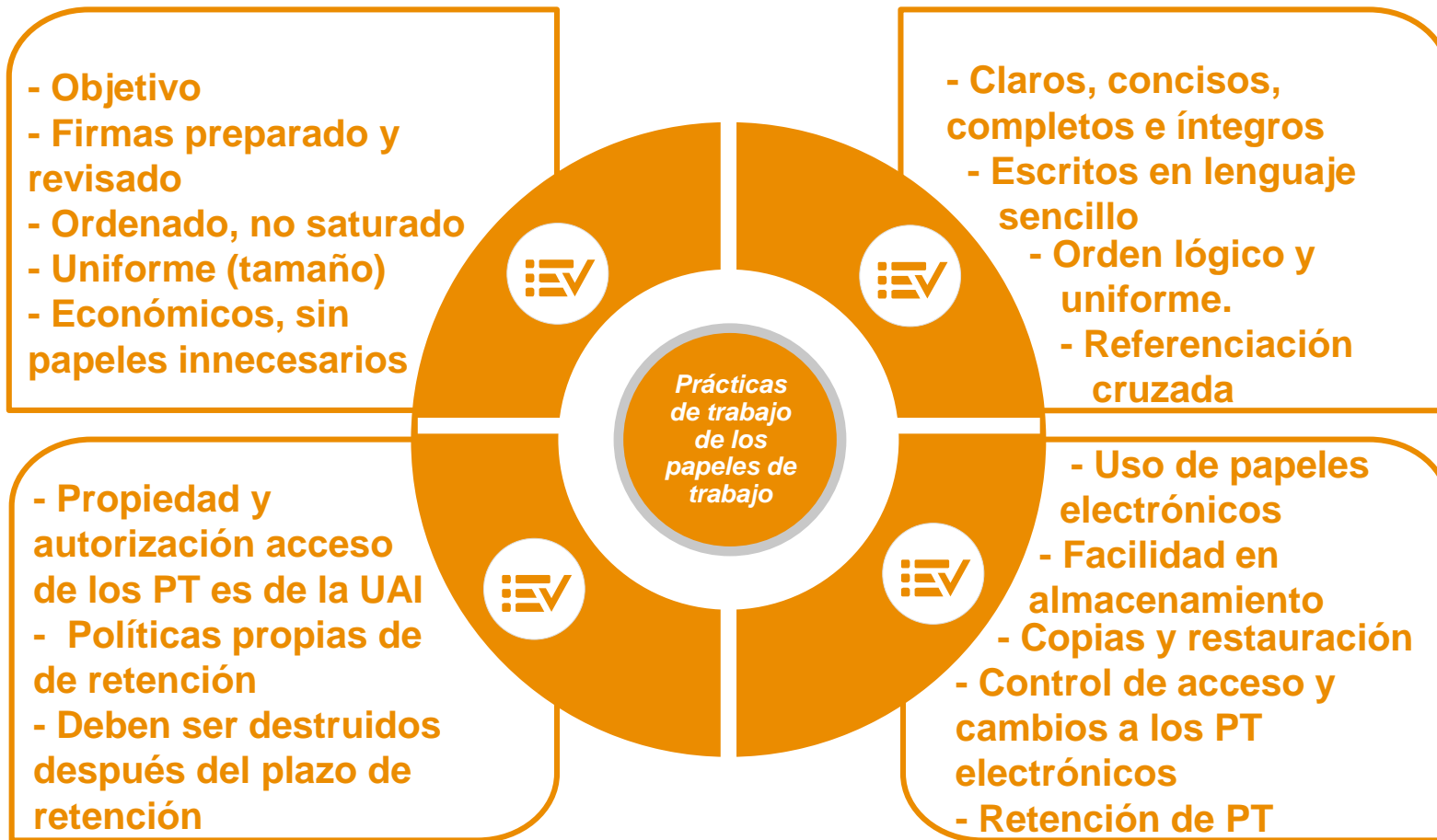
- La Dirección de auditoría interna debe revisar los papeles de trabajo preparados por el equipo de auditores.
- La Dirección de mantener el control de acceso y cambios de los papeles de trabajo.

Documentación y archivo

- La documentación incluye todo el proceso de la actividad de auditoría interna (desde planificación hasta comunicación de resultados).
- La retención de los papeles de trabajo puede ser realizada en medios físicos o medios electrónicos.

2.12 Prácticas para la preparación de papeles de trabajo

NIEPAI 2330



2.13 Cualidades de la información de los papeles de trabajo (PT)

NIEPAI 2310

S
uficiente

Es adecuada y convincente, otra persona objetivamente sacaría las mismas conclusiones que el auditor. La objetividad se mejora cuando las muestras se obtienen estadísticamente, y cuando la evidencia tiene un alto grado de persuasión.

F
iable

Es la mejor evidencia que se puede obtener. Se refiere a que la misma fue obtenida de información independiente, utilizando procedimientos apropiados (ej. Muestreo estadístico), es documentación original, y/o puede ser verificada por otra información.

2.13 Cualidades de la información de los papeles de trabajo (PT)

NIEPAI 2310

R
elevante

Apoya a las observaciones y recomendaciones del trabajo. Esta información es coincidente con el alcance del trabajo realizado y con los resultados del mismo.

U
til

Es la información que ayuda a lograr los objetivos de la organización (crear valor para los dueños, clientes, otras partes interesadas), y que sirve para cumplir con los objetivos de la actividad de auditoría interna (agregar valor, mejorar las operaciones, y ayudar a la organización a lograr objetivos)

2.13 Cualidades de la información de los papeles de trabajo (PT)

Ejemplo

El auditor interno de una Compañía, observó que los depósitos en efectivo no son depositados diariamente de manera íntegra. Una comparación de una muestra de las listas de ingresos de efectivo confirmó que el depósito en efectivo del asiento diario es igual a las cantidades monetarias (\$) de las listas de ingreso de efectivo, pero no eran iguales a las cantidades depositadas diariamente en el Banco.

Al cierre de mes se verificó que el total de las listas de ingresos de efectivo es igual al total del monto depositado en la cuenta bancaria y al total del monto debitado en los asientos diarios en la cuenta contable “Bancos”

¿Esta información en los papeles de trabajo que cualidades tiene?

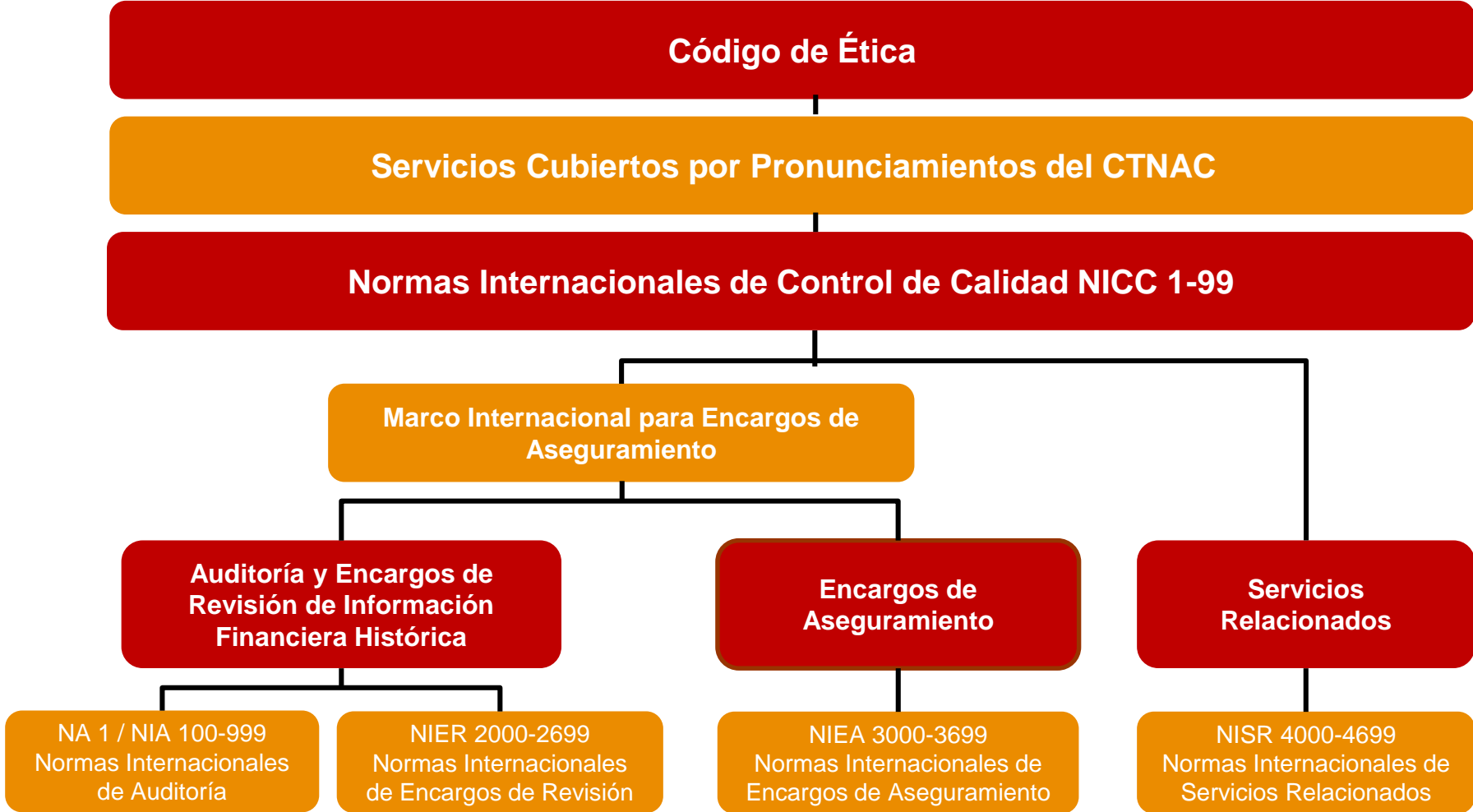
La información tiene las cualidades SFRU

3

Preparación y presentación de informes, roles, responsabilidades, y funciones del auditor interno

Informes de acuerdo con NAGA (incluye NIA)

3.1 Antecedentes para la preparación de informes (NAGA)



3.1 Antecedentes para la preparación de informes (NAGA)

Normas Internacionales de Auditoría (NIAs)	Normas Internacionales de Trabajos de Revisión (ISRE)	Normas Internacionales de Trabajos de Atestiguamiento (ISAE)
<ul style="list-style-type: none">Auditorías de Estados Financieros o información histórica	<ul style="list-style-type: none">Revisión de Estados Financieros Interinos o información histórica	<ul style="list-style-type: none">Razonabilidad (assurance) en aspectos diferentes a información financiera histórica
<ul style="list-style-type: none">Provisión de seguridad razonable	<ul style="list-style-type: none">Provisión de seguridad limitada	<ul style="list-style-type: none">Provisión de seguridad razonable o limitada

3.2 Auditorías y encargos de revisión de información financiera histórica

Auditorías

- Opinión
- Fundamento de la opinión
- Cuestiones clave de auditoría
- Responsabilidades de la gerencia y del gobierno
- Responsabilidades del auditor
- Párrafos de énfasis
- Otras cuestiones
- Empresa en marcha



Opinión sobre estados financieros



NIA 700

NIA 800



Marco contable de propósito general

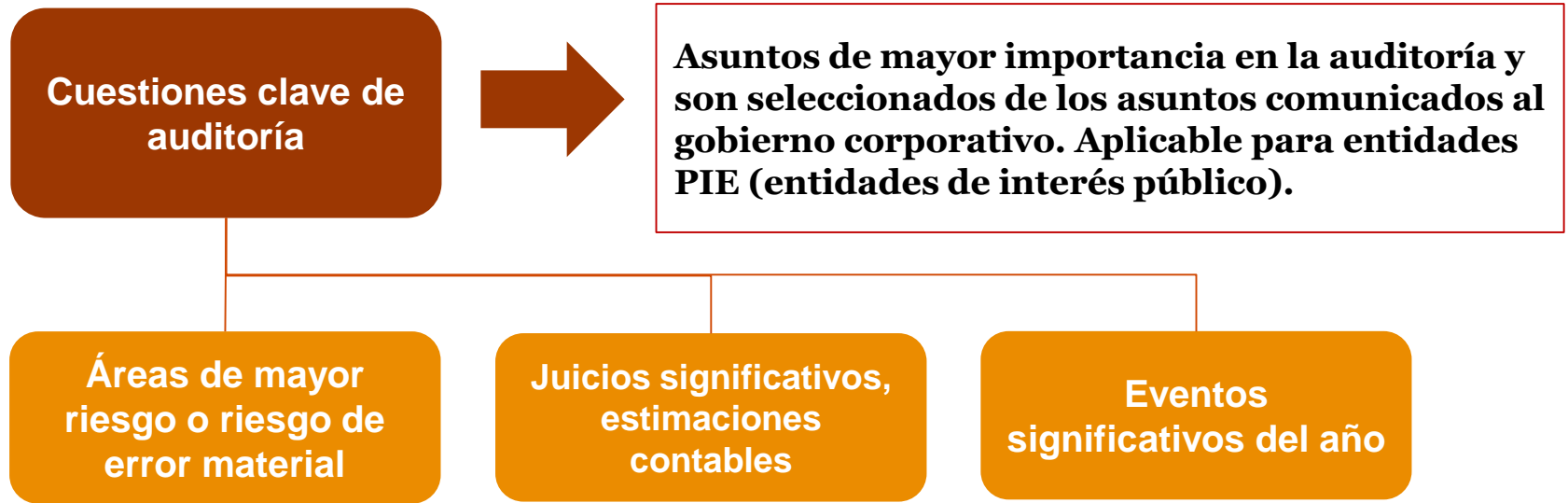
Marco contable de propósito específico



NCGA

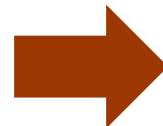
ASFI, base especial

3.2 Auditorías y encargos de revisión de información financiera histórica



Para qué se incluyen en el informe del auditor ?

- Mejoran el valor informativo del informe del auditor sobre áreas de riesgo.
- Proporcionan información asuntos que, fueron de mayor importancia en la gestión auditada.
- Ayudan a los usuarios previstos a comprender la entidad y las áreas de juicio significativo de la Gerencia en los estados financieros.



3.2 Auditorías y encargos de revisión de información financiera histórica

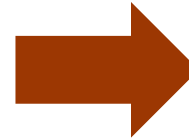
Ejemplos de posibles cuestiones clave

Se ha cambiado el sistema core de la compañía en la gestión.



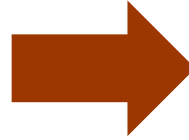
Evento del año

Se han constituido provisiones por desvalorización significativas del portafolio de inversiones de oferta privada.



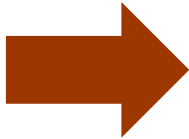
Estimación contable

En el año se han presentado pérdidas significativas por COVID-19.



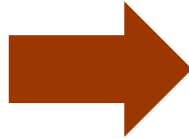
Ninguno

Se mantienen covenants por un contrato de financiamiento con la CAF que originan disparadores de prepago anticipado.



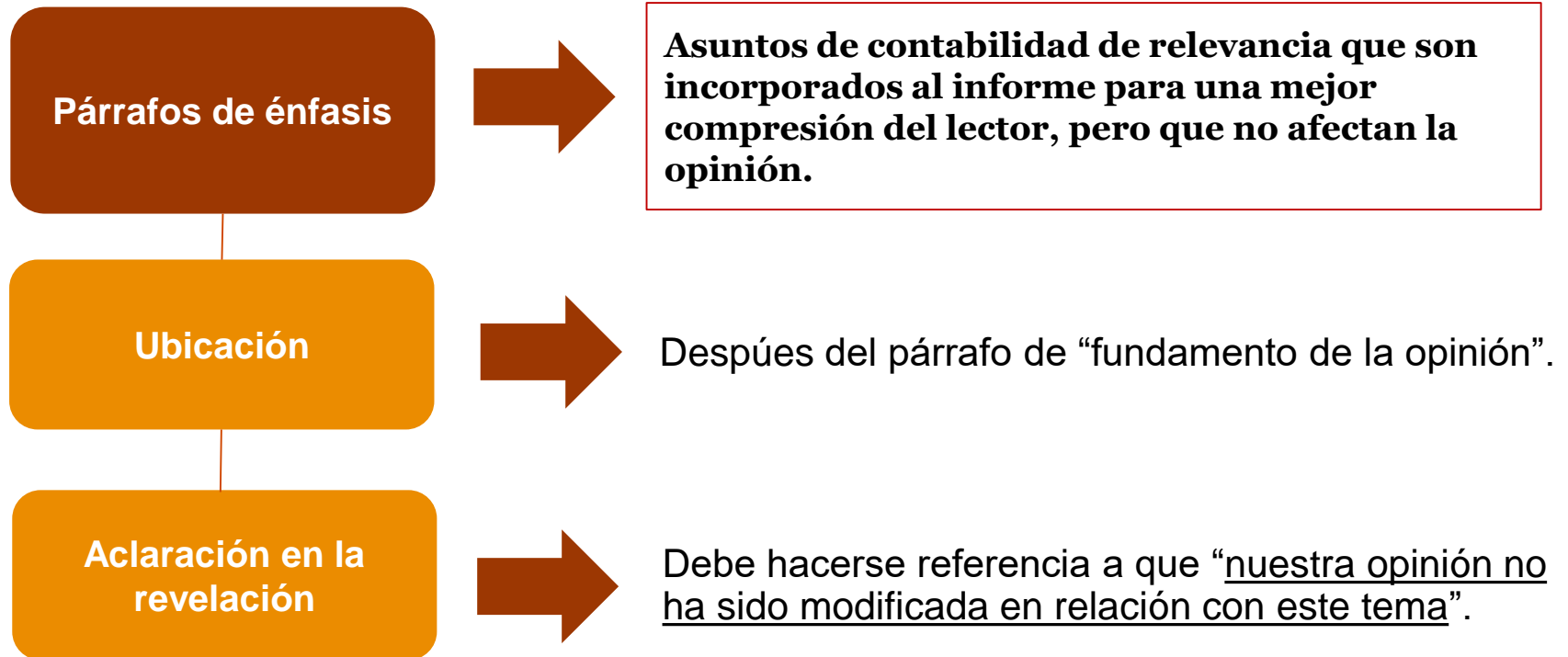
Area de riesgo

Reconocimiento de ingresos es un proceso altamente automatizado y procesa un alto volumen de transacciones.



Area de riesgo

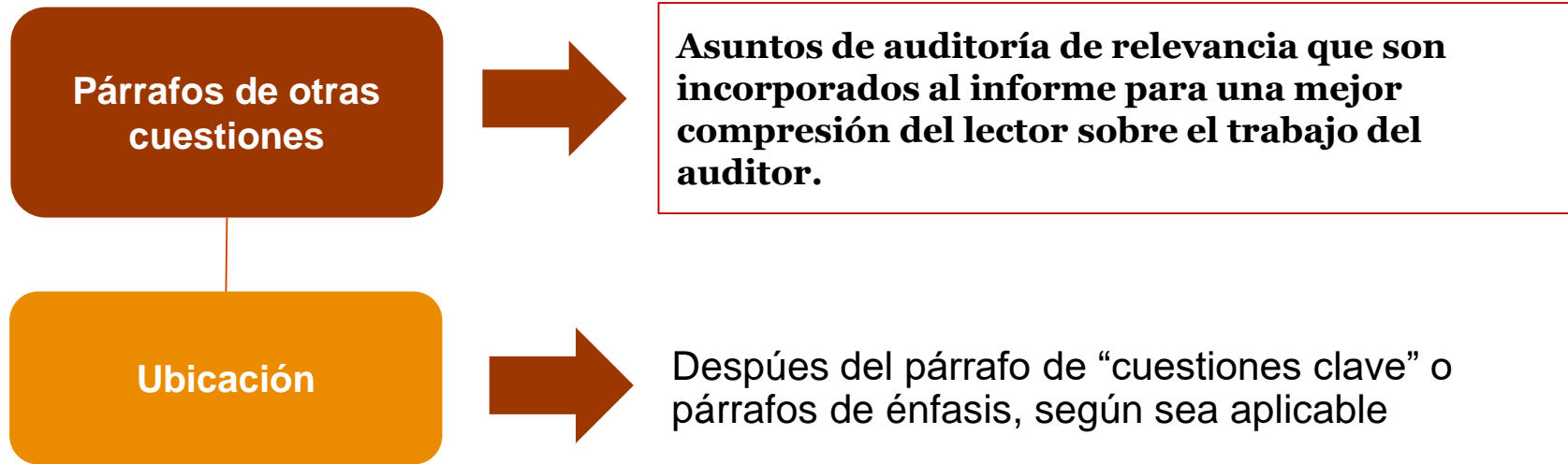
3.2 Auditorías y encargos de revisión de información financiera histórica



Ejemplos:

- Marco contable de propósito específico.
- Incertidumbre sobre empresa en marcha.
- Constitución de un deterioro.
- Recuperabilidad del CF IVA.
- Efectos del COVID-19.
- Incertidumbre sobre la resolución de un juicio.
- Hecho posterior relevante.

3.2 Auditorías y encargos de revisión de información financiera histórica



Ejemplos:

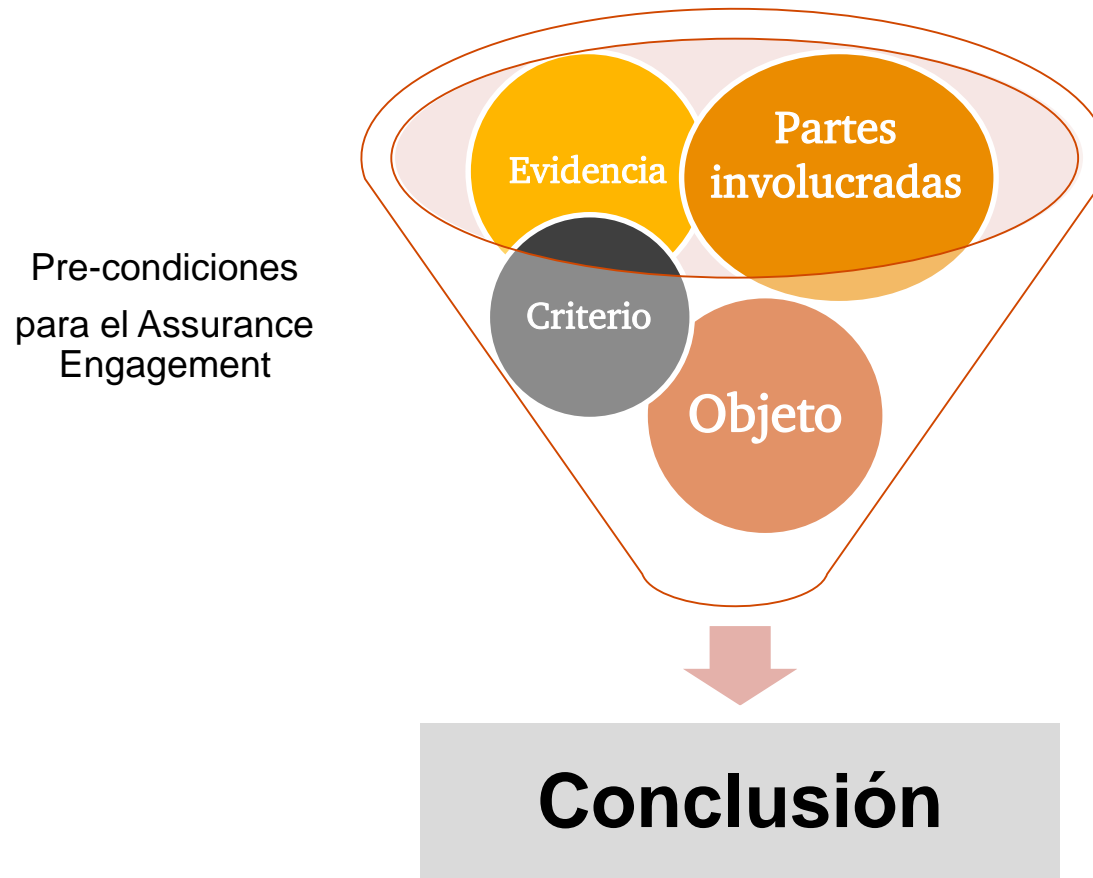
- Estado financiero auditado por otro auditor.
- Situaciones sobre las responsabilidades adicionales del auditor por la información suplementaria.
- Situaciones relevantes sobre el trabajo del auditor.
- Auditoría emitida sobre un conjunto de estados financieros que incluye información complementaria.

3.3 Encargos de aseguramiento



3.3 Encargos de aseguramiento

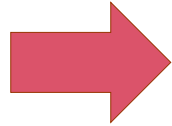
Un trabajo NAAE cuenta con los siguientes componentes:



3.3 Encargos de aseguramiento

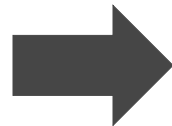
Contenido del informe

Objetivo del Engagement



Proveer aseguramiento diferente al emitido en una auditoría de EEFF o la revisión de información financiera histórica

Alcance



Deteminado por el auditor en base a los lineamientos establecidos por el objeto (client's subject matter) y el criterio establecido (criteria).

Assurance provisto



Engagements de Seguridad Razonable
Engagements de Seguridad Limitada

3.3 Encargos de aseguramiento

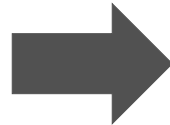
Contenido del informe

Reporting



Informe escrito conteniendo una expresión clara de la opinión/conclusión del profesional independiente, sobre la información del objeto.

Consideraciones especiales



El informe podría incluir una conclusión modificada

Distribución del informe



- Distribución restringida
- Distribución disponible para terceros determinados

Informes de acuerdo con NEPAI

3.5 Antecedentes para la preparación de informes (NEPAI)

Servicios Cubiertos por Pronunciamientos de NEPAI

Servicios de aseguramiento y cumplimiento

Examen objetivo de evidencias con el propósito de proveer una evaluación independiente de los procesos de gestión de riesgos, control y gobierno de una entidad.

Los tipos de trabajo cubiertos son:

- *Auditoría financiera.*
- *Auditoría de cumplimiento.*
- *Auditoría operativa.*
- *Auditoría de tecnologías de la información.*
- *Otros*

Trabajos de consultoría

Actividades de asesoramiento y servicios relacionados, dirigidos a añadir valor y a mejorar los procesos de gobierno, gestión de riesgos, y control de una entidad; sin que el auditor interno asuma responsabilidades de gestión.

Los tipos de trabajo cubiertos son:

- *Facilitación.*
- *Asesoramiento.*
- *Formación.*
- *Consejo.*

3.5 Antecedentes para la preparación de informes (NEPAI)

Servicios de aseguramiento y cumplimiento

Auditoría financiera

Análisis para determinar si la información financiera fue apropiadamente registrada y respaldada de manera adecuada.

Asimismo, es la evaluación sobre si las afirmaciones del desempeño de los estados financieros son razonables, precisos y fiables.

Auditoría de cumplimiento

Revisión de controles financieros y operativos para evaluar su conformidad con las leyes, normas, regulaciones, políticas, y otros requisitos establecidos.

Auditoría operativa

Evaluación de la eficacia, eficiencia y efectividad en las operaciones de una entidad.

Auditoría de TI

Evaluación de los controles y ambiente de las tecnologías de información. Entre los trabajos que se pueden realizar están:

- **Auditoría de seguridad de la información.**
- **Auditoría de seguridad del entorno de TI.**
- **Auditoría de la privacidad de la información.**

3.5 Antecedentes para la preparación de informes (NEPAI)

Servicios de aseguramiento y cumplimiento

Otros servicios de aseguramiento

Entre los principales temenos:

- **Auditorías de desempeño**, incluyen las actividades que aseguran los indicadores clave de medición del desempeño.
- **Auditorías de calidad**, incluyen actividades que aseguran que los procesos de calidad están funcionando conforme con lo previsto y que las estructuras de calidad existen.
- **Auditorías de relaciones comerciales externas**, que incluyen actividades que aseguran el cumplimiento de la relación comercial externa.
- **Auditorías de terceras partes (organización de servicios)**, incluyen las actividades que aseguran la información de un proveedor de servicios (ej. Shared service center) y el cumplimiento de las obligaciones contractuales.
- **Auditorías de contratos**, incluyen actividades que aseguran el cumplimiento de los contratos de construcción y operativos significativos y que la entidad mantiene ha suscrito con terceros.

3.6 Contenido y estructura de los informes de auditoría interna

Aspectos a considerar:

La estructura puede adecuarse a la organización y su cultura

Se tiene que ponderar al principal destinatario del reporte, para adecuar estructura y contenido

El contenido también puede adecuarse según las necesidades de los destinatarios del informe

Se tiene que considerar el uso que tendrá el reporte (ej. Para un juicio, cumplimiento regulatorio para definir la estructura y contenido

3.6 Contenido y estructura de los informes de auditoría interna

Informe de auditoría interna



1. **Título del informe del auditor**
2. **Objetivos** (propósitos del compromiso)
3. **Alcance** (actividades de auditoría, naturaleza y alcance del trabajo, limitaciones del alcance)
4. **Antecedentes** (breve resumen de la actividad auditada o explicación del proceso)



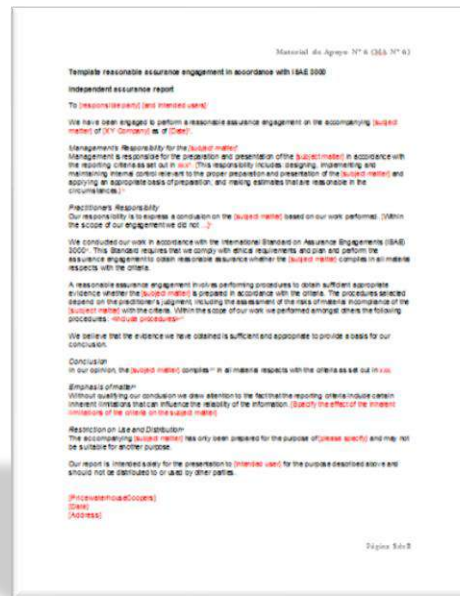
5. **Registro/resultados** (aspectos positivos, cooperación del área/actividad)
6. **Rating del trabajo** (ranking del resultado del trabajo)



7. **Conclusiones** (resumen de la opinión/evaluación del compromiso, si fuera aplicable, resaltando las observaciones críticas)
8. **Observaciones** (incluye el detalle de las observaciones con el título en cada una de ellas, el rating de riesgo, condición, criterio, causa, efecto/riesgo, recomendación y el plan de acción de la gerencia.
9. **Distribución** (incluye la restricción de los usuarios que tendrán acceso al reporte)

Este detalle sugerido por las guías de implementación de las NEPAI son enunciativas y pueden adecuarse en contenido o estructura.

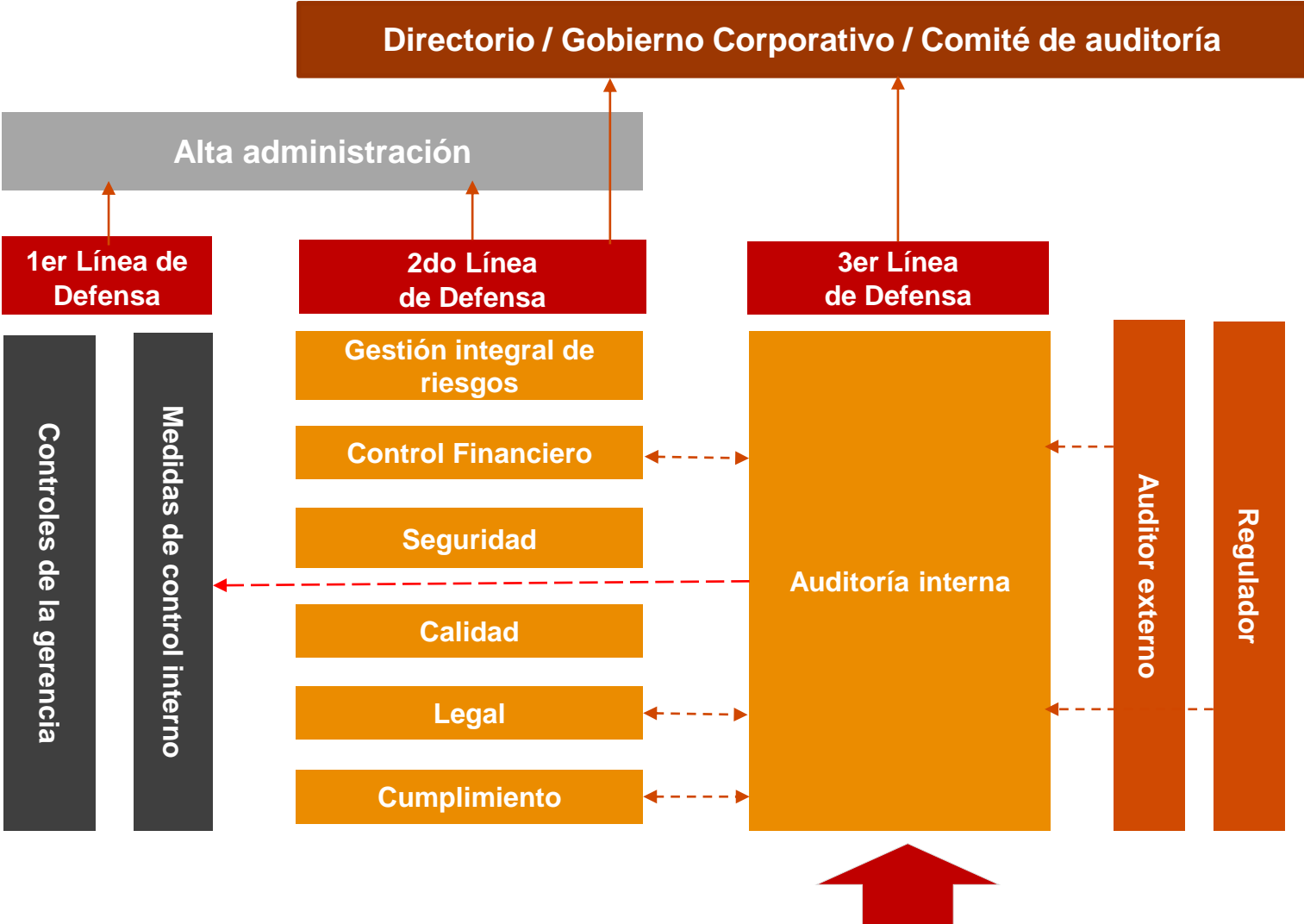
3.7 Ejemplos de modelos de informe de auditoría interna



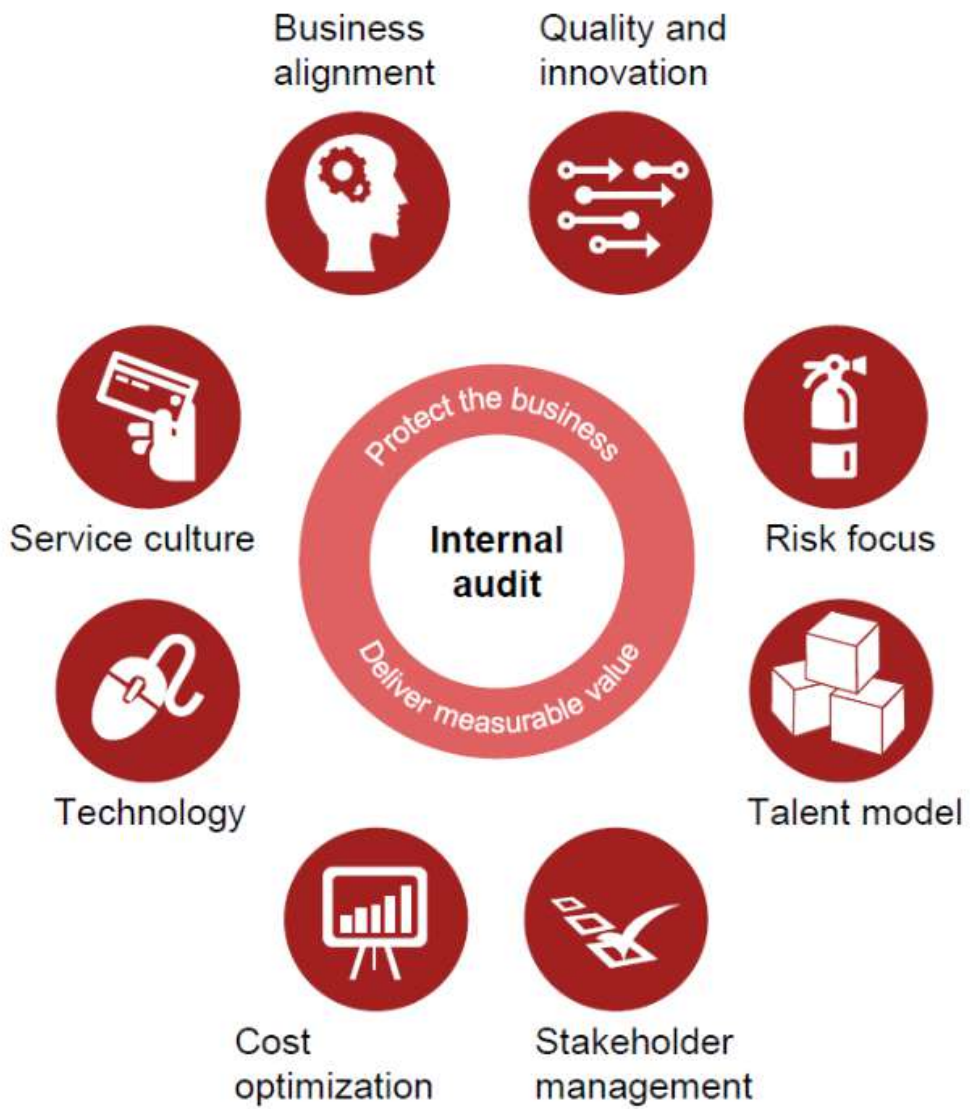
Responsabilidad y funciones del auditor interno

Roles y responsabilidades

ROLES Y RESPONSABILIDADES ESTRUCTURADAS PARA LAS TRES LINEAS DE DEFENSA



Roles y responsabilidades



Funciones

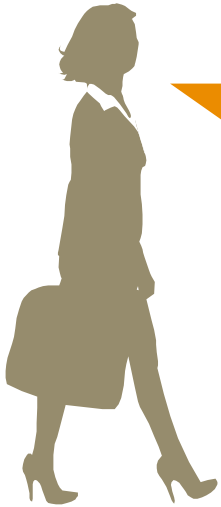
Características

Independiente y objetivo
Actitud razonablemente prudente y competente
Capacitación continua



Funciones

Es un profesional que se dedica a ayudar a las organizaciones a gestionar los riesgos al proporcionarles garantías objetivas e independientes. La auditoría interna, junto con otras funciones de gestión de riesgos dentro de la organización, desempeña un papel integral para que la organización logre sus objetivos.



Preguntas???



Gracias!!!



Gracias

[pwc.com](https://www.pwc.com)

© 2020 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.

Evaluación del Sistema de Control Interno

Programa de Capacitación - ABAV
FY2020



Agenda

01 Antecedentes

02 Componentes del control interno:

Ambiente de control (Ambiente Interno)

Evaluación de Riesgos

Actividades de control

Información y comunicación

Monitoreo (Actividades de monitoreo)

03 Pruebas de controles manuales y automáticos

04 Conclusiones

01

Antecedentes

01. ANTECEDENTES

Calentando motores...

www.menti.com

CODIGO: 24305

¿Cuándo consideras que deberíamos evaluar el control interno de la Sociedad?

¿Quién es el responsable de establecer el control interno en la Sociedad?

¿Cuál es la responsabilidad del Auditor interno ante el control interno?

01. ANTECEDENTES

Marco normativo

Reglamento de Auditores Internos
de RNMV

Autoridad de Supervisión del
Sistema Financiero (ASFI)
Recopilación de normas para
el Mercado de valores

Committee of Sponsoring
Organizations of
the Treadway Commission
(COSO)

Normas para el Ejercicio
Profesional de Auditoría
Interana (NEPAI)

Asociación de Auditoría
y Control de Sistemas
de Información
(ISACA)

Instituto de Auditores
Internos (IIA)

01. ANTECEDENTES (Cont.)

Definiciones de control interno

COSO

Según COSO el Control Interno es un proceso llevado a cabo por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y normas que sean aplicables.

ASFI VALORES

Libro 11º, Título II, Capítulo I, Sección 2, artículo 1:

Se entiende por Sistema de Control Interno al conjunto de políticas y procedimientos establecidos por la entidad supervisada, en función al tamaño y naturaleza de sus actividades, para proporcionar una seguridad razonable en el logro de los siguientes objetivos: Operativos, de información y de cumplimiento.

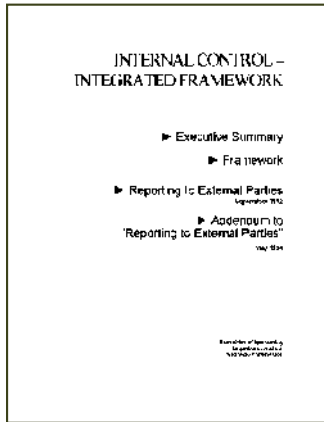
ASFI INTERMEDIACIÓN FINANCIERA

Libro 3º, Título IX, Capítulo II, Sección 2, artículo 1:

Se entiende por Sistema de Control Interno al conjunto de políticas y procedimientos establecidos por la entidad supervisada para proveer una seguridad razonable en el logro de los objetivos operativos, de información y de cumplimiento.

01. ANTECEDENTES (Cont.)

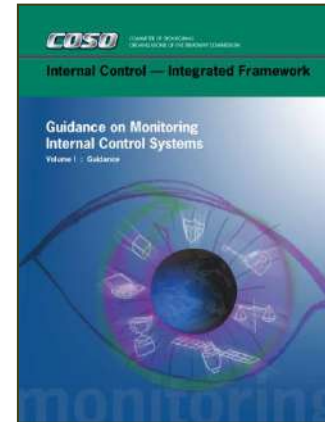
Evolución del Marco de Control Interno



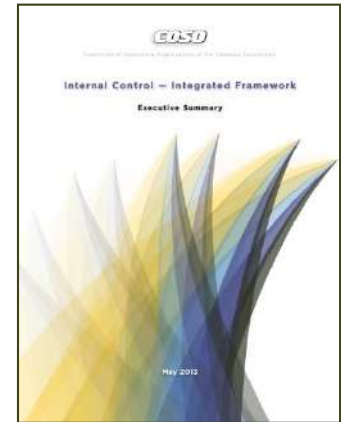
1992



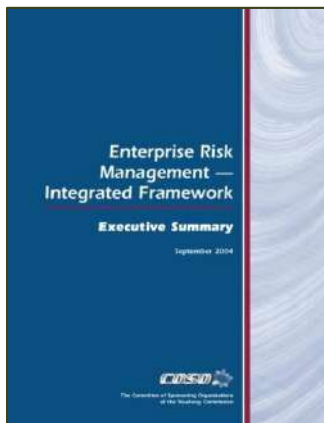
2006



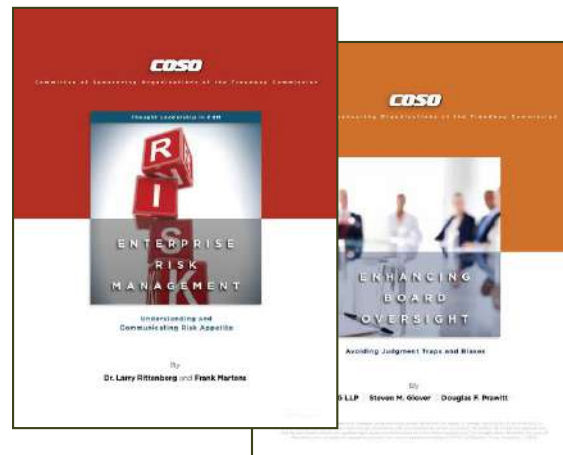
2009



2013 (Update 2017)



2004



2010



01. ANTECEDENTES (Cont.)

Responsabilidades

Directorio

Libro 11º, Título II, Capítulo I, Sección 3, artículo 1

El Directorio como **responsable máximo del establecimiento y mantenimiento** de un adecuado y efectivo Sistema de Control Interno.

Gerencia General

Libro 11º, Título II, Capítulo I, Sección 3, artículo 2

La Gerencia General **responsable de diseñar, implementar y conducir** un adecuado y efectivo Sistema de Control Interno.

Comité de Auditoría

Libro 11º, Título II, Capítulo I, Sección 4, artículo 4, inciso b.

Asegurarse que al menos una **(1) vez al año**, el Directorio revise la estructura organizacional, los manuales de procedimientos y **control interno** y de organización y funciones, así como las modificaciones de los mismos.

Auditoría interna

Libro 11º, Título II, Capítulo I, Sección 2, artículo 9:

La Unidad de Auditoría Interna será **responsable de la evaluación** del diseño, alcance y funcionamiento del Sistema de Control Interno.

01. ANTECEDENTES (Cont.)

Otros aspectos - reflexión



2010.A1 - El plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos documentada, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección y del Consejo.

2020 – Comunicación y aprobación

El director ejecutivo de auditoría debe comunicar los planes y requerimientos de recursos de la actividad de auditoría interna, incluyendo los cambios provisionales significativos, a la alta dirección y al Consejo para la adecuada revisión y aprobación. El director ejecutivo de auditoría también debe comunicar el impacto de cualquier limitación de recursos.

01. ANTECEDENTES (Cont.)

Otros aspectos - reflexión

Aspectos
que afectan
la evaluación
inicial del
control
interno

01

Cambios en los objetivos de la Sociedad

02

Cambios en la estructura organizacional de la Sociedad

03

Cambios en los procesos del negocio de la Sociedad

El 17 de marzo de 2020, el Gobierno Nacional declaró “Emergencia Sanitaria Nacional y Cuarentena” ¿Qué efectos ha tenido en la Sociedad en la que trabajan?

01. ANTECEDENTES (Cont.)

Consultas, comentarios....

TIPS....

El control interno establecido en la Sociedad es la primera línea de defensa.

El Directorio como **responsable máximo del establecimiento y mantenimiento** de un adecuado y efectivo Sistema de Control Interno.

La Gerencia General **responsable de diseñar, implementar y conducir** un adecuado y efectivo Sistema de Control Interno.

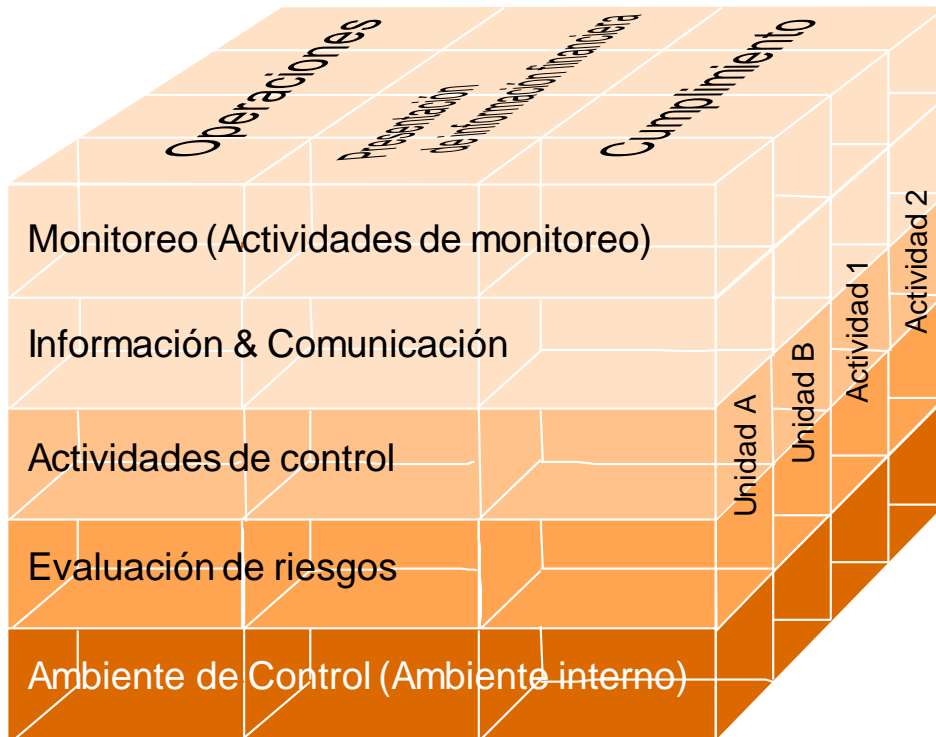
La Unidad de Auditoría Interna será **responsable de la evaluación** del diseño, alcance y funcionamiento del Sistema de Control Interno.

Los informes de la Unidad de Auditoría Interna deben identificar las debilidades exactas de control y los factores de riesgo que necesitan ser considerados....

02

Componentes del control interno

02. COMPONENTES DEL CONTROL INTERNO



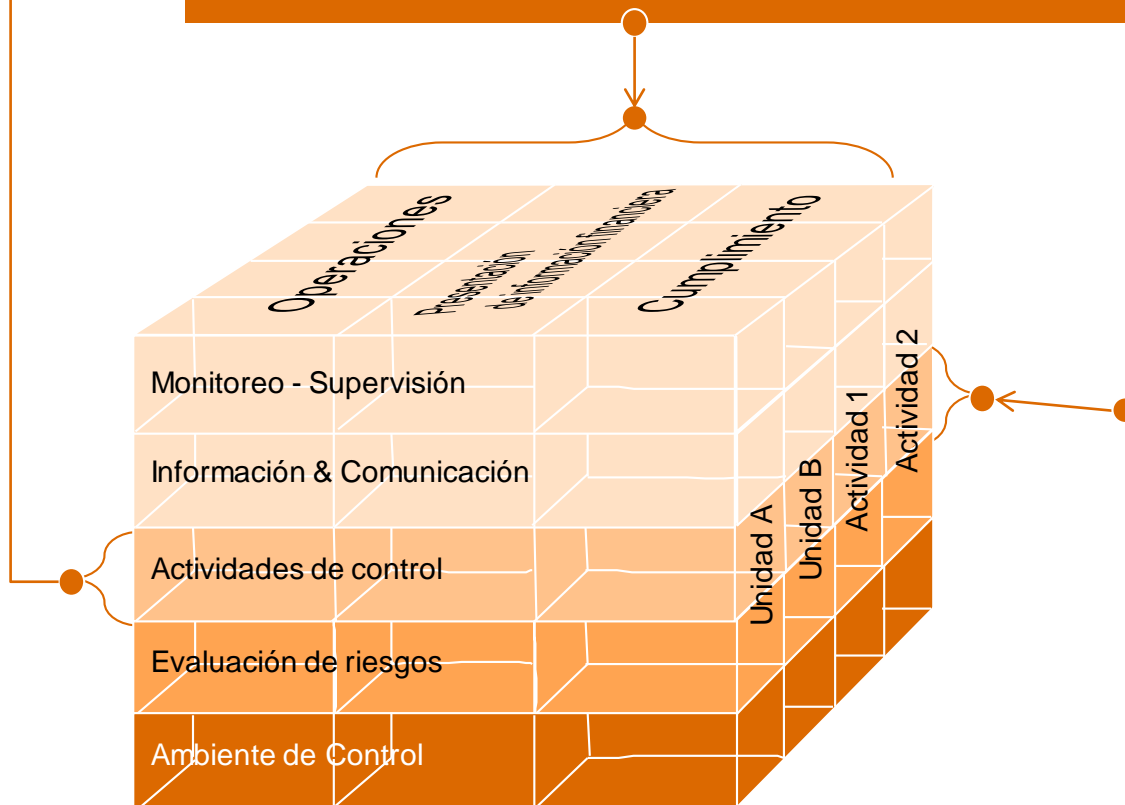
Objetivos del control interno

- Eficiencia y eficacia de las operaciones
- Confiabilidad de la información financiera
- Cumplimiento de leyes y regulaciones que sean aplicables

Se han establecido 17 principios que representan los conceptos fundamentales asociados a cada componente.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Las actividades de control son políticas y procedimientos que ayudan a garantizar que las directivas de la gerencia sean llevadas a cabo



Las actividades de control se dan a lo largo de toda la organización, en todos los niveles y en todas las funciones

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Principios

Ambiente de control (Ambiente interno)	<ol style="list-style-type: none">1. Demuestra compromiso con la integridad y valores éticos2. Ejerce responsabilidad de Supervisión3. Establece estructura, autoridad y responsabilidad4. Demuestra compromiso a la competencia5. Demanda responsabilidad
Evaluación de riesgos	<ol style="list-style-type: none">6. Especifica objetivos adecuados7. Identifica y analiza el riesgo8. Evalúa el riesgo de fraude9. Identifica y analiza cambios significativos
Actividades de control	<ol style="list-style-type: none">10. Selecciona y desarrolla actividades de control11. Selecciona y desarrolla controles generales sobre tecnología12. Las despliega mediante políticas y procedimientos
Información y comunicación	<ol style="list-style-type: none">13. Utiliza información relevante14. Se comunica a lo interno15. Se comunica a lo externo
Actividades de monitoreo	<ol style="list-style-type: none">16. Conduce evaluaciones continuas y/o separadas17. Evalúa y comunica las deficiencias

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ejercicio.... (Ver documento Anexo 1)

Grupo 1 – Ambiente de Control

Grupo 2 – Evaluación de Riesgos

Grupo 3 – Actividades de control

Grupo 4 – Información y comunicación

Grupo 5 – Monitoreo

15 minutos

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de control– Principios



1. La Sociedad demuestra un compromiso con la integridad y los valores éticos.
2. El Directorio demuestra independencia de la gerencia y ejerce la supervisión del desarrollo y desempeño del control interno.
3. La Gerencia establece, con supervisión de la junta, estructuras, líneas de informes y autoridades y responsabilidades apropiadas en la búsqueda de objetivos.
4. La Sociedad demuestra un compromiso para atraer, desarrollar y retener individuos competentes en alineación con los objetivos.
5. La Sociedad mantiene control de las personas por sus responsabilidades de control interno en la búsqueda de objetivos.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de Control– Principio #1

La Sociedad demuestra un compromiso con la integridad y los valores éticos.

Establece el “tone at the top”: la junta directiva y la gerencia en todos los niveles de la Sociedad demuestran a través de sus directivas, acciones y comportamiento la importancia de la integridad y los valores éticos para respaldar el funcionamiento del sistema de control interno.

Establece estándares de conducta: las expectativas de la junta directiva y la alta gerencia con respecto a la integridad y los valores éticos se definen en los estándares de conducta de la entidad y se entienden en todos los niveles de la organización y por los proveedores de servicios externos y socios comerciales.

Evalúa el cumplimiento de las normas de conducta: existen procesos para evaluar el desempeño de las personas y los equipos con respecto a las normas de conducta esperadas de la entidad.

Aborda las desviaciones de manera oportuna: las desviaciones de los estándares de conducta esperados de la entidad se identifican y corrigen de manera oportuna y coherente.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de Control– Principio #2

El Directorio demuestra independencia de la gerencia y ejerce la supervisión del desarrollo y desempeño del control interno.

Establece responsabilidades de supervisión: la junta directiva identifica y acepta sus responsabilidades de supervisión en relación con los requisitos y expectativas establecidos.

Aplica experiencia relevante: la junta directiva define, mantiene y evalúa periódicamente las habilidades y la experiencia necesarias entre sus miembros para permitirles hacer preguntas de sondeo a la alta gerencia y tomar medidas proporcionales.

Funciona de manera independiente: la junta directiva tiene suficientes miembros que son independientes de la gerencia y objetivos en las evaluaciones y la toma de decisiones.

Proporciona supervisión para el sistema de control interno: la junta directiva conserva la responsabilidad de supervisión del diseño, la implementación y la conducción del control interno de la gerencia.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de Control– Principio #3

La Gerencia establece, con supervisión de la junta, estructuras, lineamientos de informes y autoridades y responsabilidades apropiadas en la búsqueda de objetivos.

Considera todas las estructuras de la entidad: la gerencia y la junta directiva consideran las múltiples estructuras utilizadas (incluidas las unidades operativas, las entidades legales, la distribución geográfica y los proveedores de servicios subcontratados) para apoyar el logro de los objetivos.

Establece lineamientos de informes: la administración diseña y evalúa los lineamientos de informes para la estructura de cada entidad para permitir la ejecución de autoridades y responsabilidades y el flujo de información para administrar las actividades de la entidad.

Define, asigna y limita las autoridades y responsabilidades: la administración y la junta directiva delegan autoridad, definen responsabilidades, usan procesos y tecnología apropiados para asignar responsabilidades y segregan los deberes según sea necesario en los diversos niveles de la organización, incluida la junta directiva, altos ejecutivos Gestión, gestión, personal y proveedores de servicios subcontratados.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de Control– Principio #4

La Sociedad demuestra un compromiso para atraer, desarrollar y retener individuos competentes en alineación con los objetivos.

Establece políticas y prácticas: las políticas y prácticas reflejan las expectativas de competencia de la organización necesarias para apoyar el logro de los objetivos.

Evalúa la competencia y aborda las deficiencias: la junta directiva y la gerencia evalúan la competencia en toda la organización y en los proveedores de servicios subcontratados en relación con las políticas y prácticas establecidas, y actúa según sea necesario para abordar las deficiencias.

Atrae, desarrolla y retiene a las personas: la organización proporciona la tutoría y la capacitación necesarias para atraer, desarrollar y retener suficiente personal competente y proveedores de servicios externos para apoyar el logro de los objetivos.

Planes y preparación para la sucesión: la alta gerencia y la junta directiva desarrollan planes de contingencia para asignaciones de responsabilidad importantes para el control interno.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de Control– Principio #5

La Sociedad mantiene control de las personas por sus responsabilidades de control interno en la búsqueda de objetivos.

Aplica la rendición de cuentas a través de estructuras, autoridades y responsabilidades: la gerencia y la junta directiva establecen los mecanismos para comunicar y responsabilizar a las personas por el desempeño de las responsabilidades de control interno en toda la organización e implementar medidas correctivas según sea necesario.

Establece medidas de desempeño, incentivos y recompensas: la gerencia y la junta directiva establecen medidas de desempeño, incentivos y otras recompensas apropiadas para las responsabilidades en todos los niveles de la entidad, que reflejan las dimensiones apropiadas de desempeño y los estándares de conducta esperados, y consideran el logro de objetivos a corto y largo plazo.

Evalúa medidas de desempeño, incentivos y recompensas por relevancia continua: la gerencia y la junta directiva alinean los incentivos y recompensas con el cumplimiento de las responsabilidades de control interno en el logro de los objetivos.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Ambiente de Control– Principio #5 (Continuación)

La Sociedad mantiene control de las personas por sus responsabilidades de control interno en la búsqueda de objetivos.

Considera presiones excesivas: la administración y la junta directiva evalúan y ajustan las presiones asociadas con el logro de los objetivos a medida que asignan responsabilidades, desarrollan medidas de desempeño y evalúan el desempeño.

Evalúa el desempeño y las recompensas o disciplina a las personas: la administración y la junta directiva evalúan el desempeño de las responsabilidades de control interno, incluida la adherencia a los estándares de conducta y los niveles esperados de competencia y proporcionan recompensas o ejercen medidas disciplinarias según corresponda.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Evaluación de riesgos - Principios



6. La Sociedad especifica objetivos con suficiente claridad para permitir la identificación y evaluación de riesgos relacionados con los objetivos.
7. La Sociedad identifica los riesgos para el logro de sus objetivos en toda la entidad y analiza los riesgos como base para determinar cómo deben gestionarse los riesgos.
8. La Sociedad considera el potencial de fraude al evaluar los riesgos para el logro de los objetivos.
9. La Sociedad identifica y evalúa los cambios que podrían afectar significativamente el sistema de control interno.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Evaluación de riesgos – Principio 6

La Sociedad especifica objetivos con suficiente claridad para permitir la identificación y evaluación de riesgos relacionados con los objetivos.

Objetivos de informes financieros externos

Cumple con las normas contables aplicables: los objetivos de información financiera son consistentes con los principios contables adecuados y disponibles para esa entidad. Los principios contables seleccionados son apropiados en las circunstancias.

Considera la materialidad: la gerencia considera la materialidad en la presentación de los estados financieros.

Refleja las actividades de la entidad: los informes externos reflejan las transacciones y eventos subyacentes para mostrar características y afirmaciones cualitativas.

Tenga en cuenta que existen puntos de enfoque adicionales para informes externos no financieros, informes internos, operaciones y cumplimiento

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Evaluación de riesgos – Principio 7

La Sociedad identifica los riesgos para el logro de sus objetivos en toda la entidad y analiza los riesgos como base para determinar cómo deben gestionarse los riesgos.

Incluye los niveles de entidad, subsidiaria, división, unidad operativa y funcional: la organización identifica y evalúa los riesgos en la entidad, subsidiaria, división, unidad operativa y niveles funcionales relevantes para el logro de los objetivos.

Analiza los factores internos y externos: la identificación de riesgos considera los factores internos y externos y su impacto en el logro de los objetivos.

Involucra niveles apropiados de administración: la organización implementa mecanismos efectivos de evaluación de riesgos que involucran niveles apropiados de administración.

Estimaciones de la importancia de los riesgos identificados: los riesgos identificados se analizan mediante un proceso que incluye la estimación de la importancia potencial del riesgo.

Determina cómo responder a los riesgos: la evaluación de riesgos incluye considerar cómo se debe gestionar el riesgo y si aceptar, evitar, reducir o compartir el riesgo.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Evaluación de riesgos – Principio 8

La Sociedad considera el potencial de fraude al evaluar los riesgos para el logro de los objetivos

Considera varios tipos de fraude: la evaluación del fraude considera la presentación de informes fraudulentos, la posible pérdida de activos y la corrupción como resultado de las diversas formas en que puede ocurrir el fraude y la mala conducta.

Evalúa incentivos y presiones: la evaluación del riesgo de fraude considera incentivos y presiones.

Evalúa las oportunidades: la evaluación del riesgo de fraude considera las oportunidades para la adquisición, el uso o la eliminación no autorizados de activos, la alteración de los registros de informes de la entidad o la comisión de otros actos inapropiados.

Evalúa actitudes y racionalizaciones: la evaluación del riesgo de fraude considera cómo la gerencia y otro personal pueden participar o justificar acciones inapropiadas.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Evaluación de riesgos – Principio 9

La Sociedad identifica y evalúa los cambios que podrían afectar significativamente el sistema de control interno.

Evalúa los cambios en el entorno externo: el proceso de identificación de riesgos considera los cambios en el entorno normativo, económico y físico en el que opera la entidad.

Evalúa los cambios en el modelo de negocios: la organización considera los posibles impactos de las nuevas líneas de negocios, las composiciones alteradas dramáticamente de las líneas de negocios existentes, las operaciones comerciales adquiridas o desinvertidas en el sistema de control interno, el rápido crecimiento, la dependencia cambiante de las geografías extranjeras y las nuevas tecnologías.

Evalúa los cambios en el liderazgo: la organización considera los cambios en la gestión y las actitudes y filosofías respectivas sobre el sistema de control interno

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control– Principios



10. La Sociedad selecciona y desarrolla actividades de control que contribuyen a la mitigación de riesgos para el logro de objetivos a niveles aceptables.

11. La Sociedad selecciona y desarrolla actividades de control general sobre la tecnología para apoyar el logro de los objetivos.

12. La Sociedad despliega actividades de control a través de políticas que establecen lo que se espera y procedimientos que implementan políticas.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control – Principio 10

La Sociedad selecciona y desarrolla actividades de control que contribuyen a la mitigación de riesgos para el logro de objetivos a niveles aceptables.

Se integra con la evaluación de riesgos: las actividades de control ayudan a garantizar que las respuestas a los riesgos que abordan y mitigan los riesgos se llevan a cabo.

Considera factores específicos de la entidad: la gerencia considera cómo el entorno, la complejidad, la naturaleza y el alcance de sus operaciones, así como las características específicas de su organización, afectan la selección y el desarrollo de las actividades de control.

Determina los procesos comerciales relevantes: la administración determina qué procesos comerciales relevantes requieren actividades de control.

Evalúa una combinación de tipos de actividades de control: las actividades de control incluyen una variedad y variedad de controles y pueden incluir un equilibrio de enfoques para mitigar los riesgos, teniendo en cuenta los controles manuales y automatizados, y los controles preventivos y de detección.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control – Principio 10 (Cont.)

La Sociedad selecciona y desarrolla actividades de control que contribuyen a la mitigación de riesgos para el logro de objetivos a niveles aceptables.

Considera a qué nivel se aplican las actividades: la gerencia considera las actividades de control a varios niveles en la entidad.

Aborda la segregación de deberes: la administración segrega deberes incompatibles y, cuando dicha segregación no es práctica, la gerencia selecciona y desarrolla actividades de control alternativas.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control – Principio 11

La Sociedad selecciona y desarrolla actividades de control general sobre la tecnología para apoyar el logro de los objetivos.

Determina la dependencia entre el uso de la tecnología en los procesos comerciales y los controles generales de la tecnología: la gerencia comprende y determina la dependencia y el vínculo entre los procesos comerciales, las actividades de control automatizado y los controles generales de la tecnología.

Establece actividades relevantes para el control de la infraestructura tecnológica: la gerencia selecciona y desarrolla actividades de control sobre la infraestructura tecnológica, que están diseñadas e implementadas para ayudar a garantizar la integridad, precisión y disponibilidad del procesamiento de la tecnología.

Establece actividades relevantes de control de procesos de gestión de seguridad: la gerencia selecciona y desarrolla actividades de control que están diseñadas e implementadas para restringir los derechos de acceso a la tecnología a los usuarios autorizados de acuerdo con sus responsabilidades laborales y para proteger los activos de la entidad de amenazas externas

• .

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control – Principio 11 (Cont.)

La Sociedad selecciona y desarrolla actividades de control general sobre la tecnología para apoyar el logro de los objetivos.

Establece actividades relevantes de control de procesos de adquisición, desarrollo y mantenimiento de tecnología: la gerencia selecciona y desarrolla actividades de control sobre la adquisición, el desarrollo y el mantenimiento de la tecnología y su infraestructura para lograr los objetivos de la gerencia.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control – Principio 12

La Sociedad despliega actividades de control a través de políticas que establecen lo que se espera y procedimientos que implementan políticas.

Establece políticas y procedimientos para respaldar la implementación de las directivas de la administración: la administración establece actividades de control integradas en los procesos comerciales y las actividades cotidianas de los empleados a través de políticas que establecen lo que se espera y procedimientos relevantes que especifican acciones.

Establece la responsabilidad y la rendición de cuentas por la ejecución de políticas y procedimientos: la gerencia establece la responsabilidad y la rendición de cuentas por las actividades de control con la gerencia (u otro personal designado) de la unidad o función comercial en la que residen los riesgos relevantes.

Se desempeña de manera oportuna: el personal responsable realiza actividades de control de manera oportuna según lo definido por las políticas y procedimientos.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Actividades de control – Principio 12 (Cont.)

La Sociedad despliega actividades de control a través de políticas que establecen lo que se espera y procedimientos que implementan políticas.

Toma medidas correctivas: el personal responsable investiga y actúa sobre los asuntos identificados como resultado de la ejecución de actividades de control.

Realiza el uso de personal competente: el personal competente con suficiente autoridad realiza actividades de control con diligencia y enfoque continuo.

Reevalúa las políticas y los procedimientos: la gerencia revisa periódicamente las actividades de control para determinar su relevancia continua y las actualiza cuando es necesario.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Información y comunicación - Principios



13. La Sociedad obtiene o genera y utiliza información relevante y de calidad para respaldar el funcionamiento del control interno.

14. La Sociedad comunica internamente información, incluidos objetivos y responsabilidades para el control interno, necesarios para apoyar el funcionamiento del control interno.

15. La Sociedad se comunica con partes externas con respecto a asuntos que afectan el funcionamiento del control interno.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Información y comunicación – Principio 13

La Sociedad obtiene o genera y utiliza información relevante y de calidad para respaldar el funcionamiento del control interno.

Identifica los requisitos de información: se ha implementado un proceso para identificar la información requerida y esperada para respaldar el funcionamiento de los otros componentes del control interno y el logro de los objetivos de la entidad.

Captura fuentes de datos internas y externas: los sistemas de información capturan fuentes de datos internas y externas.

Procesa datos relevantes en información: los sistemas de información procesan y transforman datos relevantes en información.

Mantiene la calidad durante todo el procesamiento: los sistemas de información producen información oportuna, actual, precisa, completa, accesible, protegida, verificable y retenida. La información se revisa para evaluar su relevancia en el soporte de los componentes de control interno.

Considera los costos y beneficios: la naturaleza, cantidad y precisión de la información comunicada son proporcionales y respaldan el logro de los objetivos.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Información y comunicación – Principio 14

La Sociedad comunica internamente información, incluidos objetivos y responsabilidades para el control interno, necesarios para apoyar el funcionamiento del control interno.

Comunica información de control interno: se ha implementado un proceso para comunicar la información requerida para que todo el personal pueda comprender y llevar a cabo sus responsabilidades de control interno.

Se comunica con la Junta Directiva: existe comunicación entre la administración y la junta directiva para que ambos tengan la información necesaria para cumplir sus funciones con respecto a los objetivos de la entidad.

Proporciona líneas de comunicación separadas: existen canales de comunicación separados, como líneas directas de denuncia de irregularidades, que sirven como mecanismos a prueba de fallas para permitir la comunicación anónima o confidencial cuando los canales normales no funcionan o no son efectivos.

Selecciona el método de comunicación relevante: el método de comunicación considera el momento, la audiencia y la naturaleza de la información.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Información y comunicación – Principio 15

La Sociedad se comunica con partes externas con respecto a asuntos que afectan el funcionamiento del control interno.

Se comunica con las partes externas: existen procesos para comunicar información relevante y oportuna a las partes externas, incluidos accionistas, socios, propietarios, reguladores, clientes y analistas financieros y otras partes externas.

Permite las comunicaciones entrantes: los canales de comunicación abiertos permiten la entrada de clientes, consumidores, proveedores, auditores externos, reguladores, analistas financieros y otros, proporcionando a la gerencia y al consejo de administración información relevante.

Se comunica con la Junta Directiva: la información relevante resultante de las evaluaciones realizadas por terceros se comunica a la Junta Directiva.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Monitoreo - Principios



16. La Sociedad selecciona, desarrolla y realiza evaluaciones continuas y / o separadas para determinar si los componentes del control interno están presentes y funcionando.

17. La Sociedad evalúa y comunica las deficiencias de control interno de manera oportuna a las partes responsables de tomar medidas correctivas, incluida la alta gerencia y la junta directiva, según corresponda.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Monitoreo – Principio 16

La Sociedad selecciona, desarrolla y realiza evaluaciones continuas y / o separadas para determinar si los componentes del control interno están presentes y funcionando.

Considera una combinación de evaluaciones continuas y separadas: la administración incluye un balance de evaluaciones continuas y separadas.

Considera la tasa de cambio: la gerencia considera la tasa de cambio en los negocios y los procesos comerciales al seleccionar y desarrollar evaluaciones continuas y separadas.

Establece la comprensión de la línea de base: el diseño y el estado actual de un sistema de control interno se utilizan para establecer una línea de base para evaluaciones continuas y separadas.

Utiliza personal con conocimientos: los evaluadores que realizan evaluaciones continuas y separadas tienen suficiente conocimiento para comprender lo que se está evaluando.

Se integra con los procesos comerciales: las evaluaciones continuas se incorporan a los procesos comerciales y se ajustan a las condiciones cambiantes.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Monitoreo – Principio 16 (Cont.)

La Sociedad selecciona, desarrolla y realiza evaluaciones continuas y / o separadas para determinar si los componentes del control interno están presentes y funcionando.

Ajusta el alcance y la frecuencia: la administración varía el alcance y la frecuencia de evaluaciones separadas según el riesgo.

Evalúa objetivamente: se realizan evaluaciones separadas periódicamente para proporcionar retroalimentación objetiva.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Monitoreo – Principio 17

La Sociedad evalúa y comunica las deficiencias de control interno de manera oportuna a las partes responsables de tomar medidas correctivas, incluida la alta gerencia y la junta directiva, según corresponda.

Evalúa los resultados: la administración y la junta directiva, según corresponda, evalúan los resultados de evaluaciones continuas y separadas.

Comunica las deficiencias: las deficiencias se comunican a las partes responsables de tomar medidas correctivas y a la alta gerencia y la junta directiva, según corresponda.

Supervisa las acciones correctivas: la administración rastrea si las deficiencias se corrigen de manera oportuna.

02. COMPONENTES DEL CONTROL INTERNO (Cont.)

Consultas, comentarios....

TIPS....

Debemos documentar nuestra evaluación de riesgos por lo menos una vez al año.

Los cambios en procesos, personas que ejecutan los controles nos tienen que llamar la atención para evaluar en qué medida afectan en el sistema de control interno de la Sociedad.

No debemos perder de vista que una buena evaluación del sistema del control interno nos permitirá identificar puertas por donde los riesgos pueden materializarse.

3

Pruebas de
controles
manuales
y automáticos

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

OBJETIVOS

Reconocer la importancia del entendimiento del proceso para identificar controles

Documentación suficiente para documentar nuestro entendimiento de los controles

Identificar y responder a deficiencias de controles

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

TIPOS DE CONTROLES

Frecuencia

- Anual
- Mensualmente
- Semanal

Objetivo

- Detectivo
- Preventivo

Dependencia de TI

- Manual
- Manual dependiente de TI
- Automático e ITGC

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

1. Entender el proceso de inicio a fin identificando riesgos potenciales de error

2. Identificar controles clave y evaluar su diseño e implementación

3. Testeo de controles y consideración de otra evidencia que respalde su efectividad operativa

4. Identificar y responder a deficiencias de control

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Entender el proceso de inicio a fin identificando riesgos potenciales de error

Si no cumplimos con este paso, podemos:

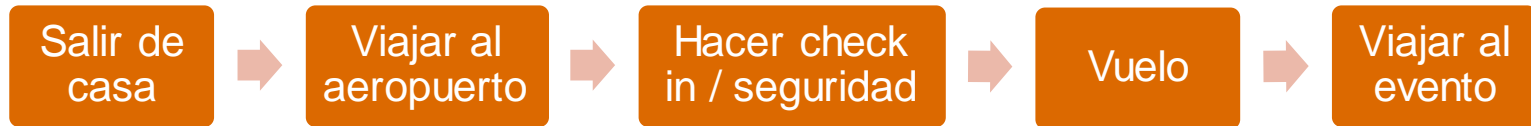
- Fallar en identificar riesgos.
- Fallar en evaluar el diseño e implementación de controles.
- Fallar en diseñar procedimientos de respuesta de auditoria en respuesta a esos riesgos.

Finalmente, puede que no obtengamos suficiente evidencia para respaldar nuestros resultados respecto a las pruebas de control

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Entender el proceso de inicio a fin identificando riesgos potenciales de error

“El viaje”

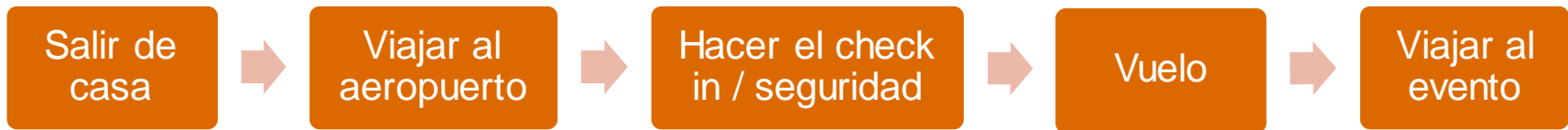


Asistir a un evento a 400 kilómetros de casa en una fecha y hora específica en el futuro.

¿Qué podría salir mal?

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Entender el proceso de inicio a fin identificando riesgos potenciales de error



- ✱ Desorganización (ej. Maleta sin hacer)

- ✱ Quedarse dormido

- ✱ Interrupciones

- ✱ Taxi atrasado

- ✱ Tráfico

- ✱ El auto se avería

- ✱ Perderse

- ✱ Largas filas

- ✱ Olvidar el pasaporte / cédula

- ✱ Seleccionado para una inspección de seguridad adicional

- ✱ El vuelo está retrasado

- ✱ La tripulación está atrasada

- ✱ Mal clima

- ✱ Tráfico en la pista

- ✱ Equipaje perdido

- ✱ Taxi atrasado

- ✱ El auto se avería

- ✱ Perderse

Los riesgos potenciales de error, deben contar con un control que minimicen su efecto.

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Procesos de negocio

- Tesorería – Caja e Inversiones
- Ingresos y Cuentas por cobrar
- Reporte financiero de cierre del período
- Administración de Fondos
- Inversiones (Valuación, devengamiento)
- Comisiones por intermediación (Compra, venta de títulos)

Entendimiento en lo aplicable

- Entender los procedimientos por el cual se inician las transacciones, son autorizadas, procesadas, registradas y reportadas;
- Entender - registros contables relacionados, información de respaldo y cuentas específicas que se utilizan
- Entender - ¿Cómo el sistema de información captura los eventos y transacciones que no sean transacciones habituales
- Entender - el proceso de reporte financiero al cierre del período (cierre contable).

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Tips para documentar el entendimiento del control

Documentar

- Narrativo.
- Flujograma.
- Flujograma narrado.

NEPAI

2330 – Documentación de la información

Los auditores internos deben documentar información suficiente, fiable, relevante, y útil que les permita respaldar los resultados del trabajo y las conclusiones.

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Tips para documentar el entendimiento del control

Input	Process/Control	Output	Number	Description
<p>2.1 Transacciones en caja</p> <p>Retiro de efectivo</p>			<p>2.1</p> <p>2.1.1</p>	<p>Las operaciones en caja comienza a horas 8:30, los cajeros durante el día pueden realizar las siguientes operaciones:</p> <ul style="list-style-type: none"> * Pago de préstamo * Retiro * Depósitos - Apertura de caja de ahorro * Pago de servicios * Giros Nacionales * Transferencias al exterior <p>Retiros de efectivo</p> <p>El cajero mediante ticket llama al cliente, una vez en cajas, consulta que operación realizara posteriormente solicita el ticket, carnet del cliente, libreta de ahorro o el N° de la cuenta de la caja de ahorro, y la huella digital de su dedo índice del cliente , una vez reconocida la huella digital, introduce el N° de la cuenta de caja de ahorro y el importe a retirar, una vez realizado esto el cajero procede a entregar el efectivo y emitir el voucher para que sea firmado por el cliente, posteriormente el cajero entrega una copia de su voucher y la actualización de la libreta de ahorro.</p> <p>Los retiros por el cliente pueden ser realizados con la libreta de ahorro o sin la libreta de ahorro, en caso de no contar con el N° de la caja de ahorro el cliente se debe apersonar a Plataformas.</p> <p>BCA- 017: El "Cajero" verifica el carnet de identidad, la firma, la huella digital del dedo índice o medio en el sistema, para proceder con el retiro de efectivo de la caja de ahorro.</p> <p>Los retiros de efectivo son registrados automáticamente en el sistema xxxx, el mismo es realizado mediante un proceso BATCH y es visualizado en el sistema al día siguiente.</p> <p>BCA- 018: El sistema xxxx registra automáticamente los retiros efectuados por el cliente en cajas, el mismo es realizado mediante un proceso BATCH y es visualizado en el sistema al día siguiente.</p>

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

1. Entender el proceso de inicio a fin identificando riesgos potenciales de error

2. Identificar controles clave y evaluar su diseño e implementación

3. Testeo de controles y consideración de otra evidencia que respalde su efectividad operativa

4. Identificar y responder a deficiencias de control

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Proceso vs Control

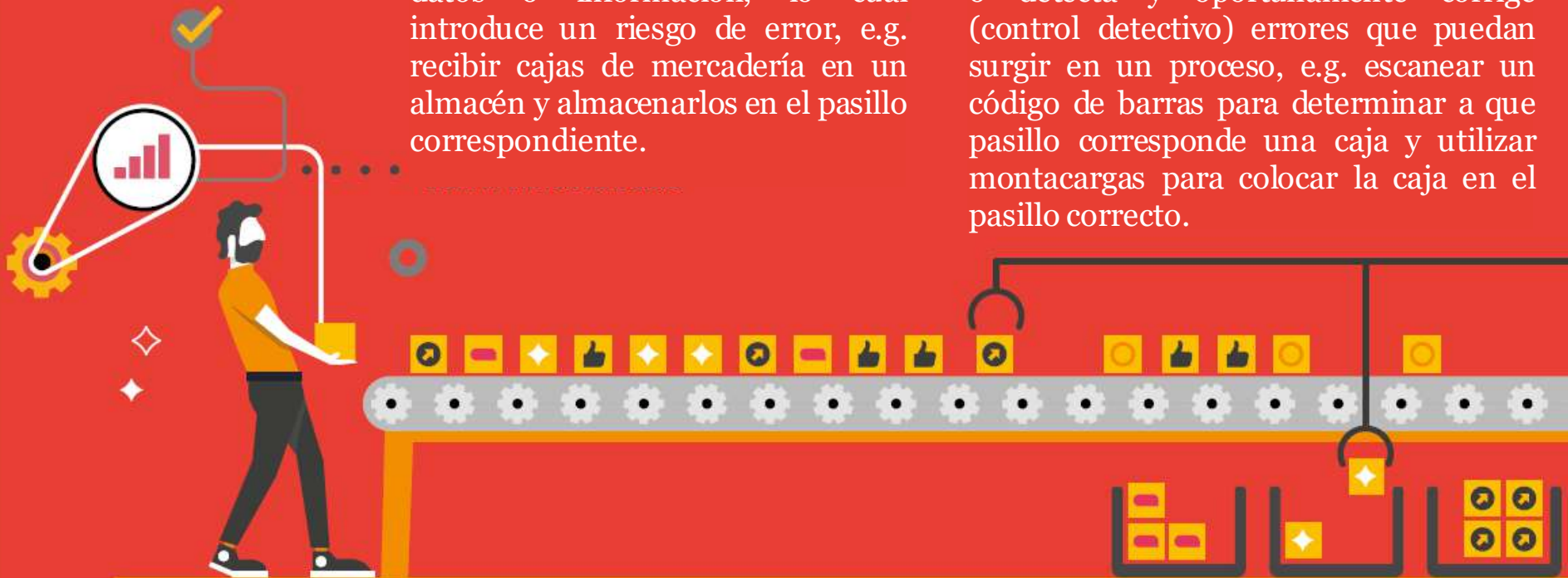
Proceso:

Un proceso cambia o transforma datos o información, lo cual introduce un riesgo de error, e.g. recibir cajas de mercadería en un almacén y almacenarlos en el pasillo correspondiente.

© iStockphoto.com/Andreas Galle

Control:

Un control previene (control preventivo) o detecta y oportunamente corrige (control detectivo) errores que puedan surgir en un proceso, e.g. escanear un código de barras para determinar a que pasillo corresponde una caja y utilizar montacargas para colocar la caja en el pasillo correcto.



03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

- La existencia de diferencias entre los controles documentados y los realmente implementados puede ser más común que lo esperado.
- Los cambios a los negocios o a los procesos que impactan riesgos son difíciles de identificar cuando solamente revisamos documentación.
- Los walkthroughs (pruebas de recorrido) necesitan ser planeados apropiadamente, llevados a cabo con el debido cuidado y con un nivel de escepticismo profesional, y nuestra documentación debe reflejar que:
 - Realizamos indagaciones al personal que en realidad lleva a cabo las actividades, no solamente a los supervisores
 - Corroborar respuestas a indagaciones (p.e.: inspeccionar documentos o registros contables o realizar indagaciones cruzadas para corroborar con otro personal)

Será Control clave el control que nos proporciona mayor evidencia de auditoría

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

1. Entender el proceso de inicio a fin identificando riesgos potenciales de error

2. Identificar controles clave y evaluar su diseño e implementación

3. Testeo de controles y consideración de otra evidencia que respalde su efectividad operativa

4. Identificar y responder a deficiencias de control

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Técnicas para el testeo de controles

Reproceso

Ponerse en los zapatos del ejecutor y reprocesar el control según lo diseñado

Inspección

Inspección de la evidencia de control

Observación

Observar cómo el propietario del control realiza el procedimiento de control

Indagaciones

Entrevistar a quién realiza el control o al gerente responsable

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Muestreo

Consejo para la práctica 2330-3

Estadístico

No Estadístico

Muestreo aleatorio: cada elemento de la población tiene la misma probabilidad de ser seleccionado para la muestra y no contempla condiciones predeterminadas. Este es el concepto en el que se basa la herramienta “sampling” en Excel.

Muestreo por unidades monetarias: utilizado para identificar errores monetarios en “sumas y saldos” de una cuenta de balance; por ejemplo, revisando el saldo de cuentas por cobrar, el auditor interno podría seleccionar las partidas particulares de mayor monto, para lograr mayor cobertura en términos monetarios.

Muestreo por atributos: utilizado para determinar las características de una población; por ejemplo, seleccionar sólo las existencias con saldo positivo las cuales representan los artículos que deben existir y estar disponibles para la venta.



03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Tips para determinación muestra

Estadístico

Ejemplo.

<i>Frecuencia de control</i>	<i>Población asumida de ocurrencias de control</i>	<i>Número de ítems a probar</i>	
		<i>Seguridad elevada</i>	<i>Seguridad moderada</i>
Anual	1	1	1
Trimestral	4	2	1
Mensual	12	2	2
Semanal	52	5	4
Diario	250	20	10
Varias veces por día	Más de 250	25	15

Fuentes: American Association of Public Accountants (AICPA) **Audit sampling guidance for compliance audits.**

Appendix A – Attributes statistical sampling tables

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Reflexionemos

Definición de excepciones

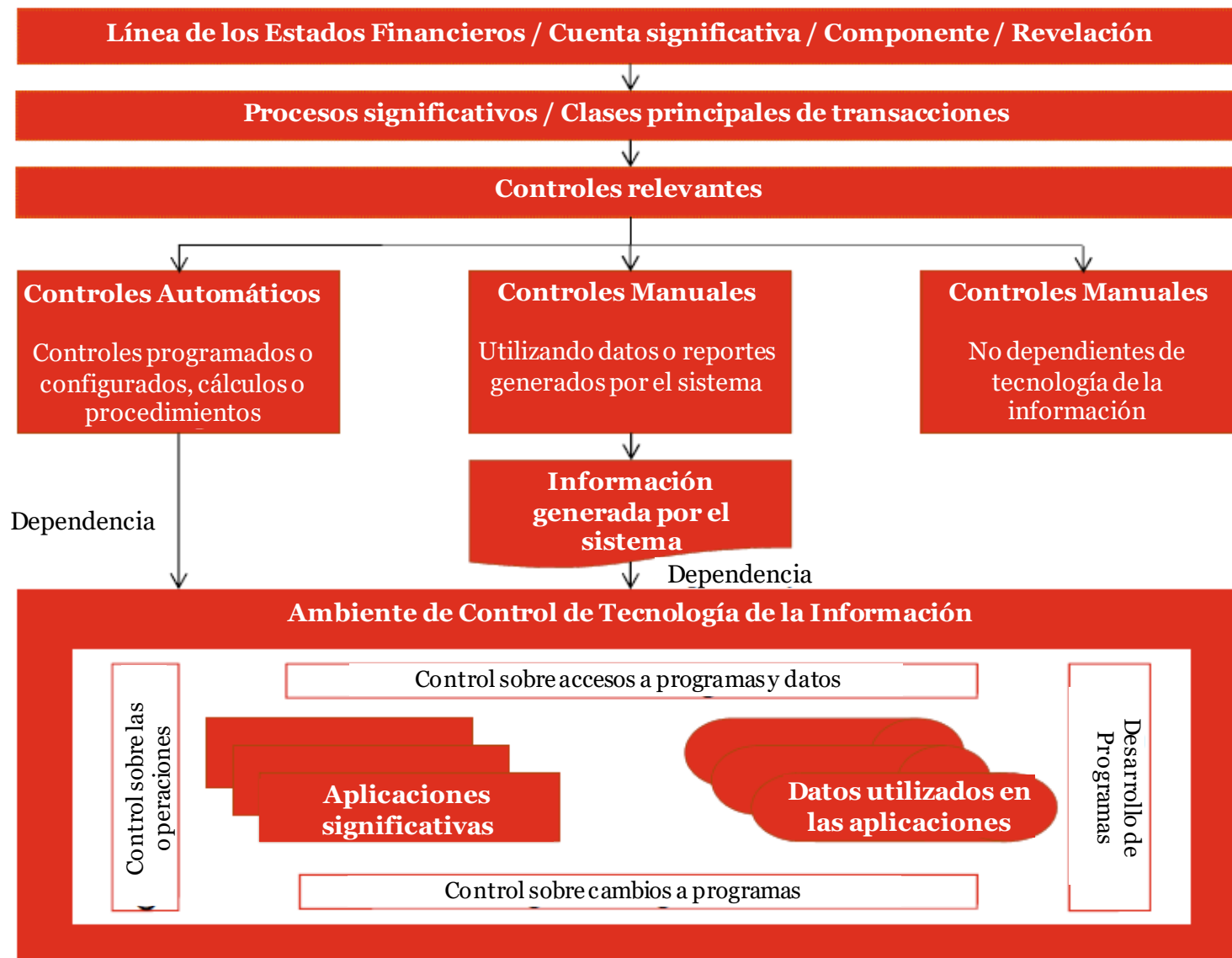
Población a probar

El IIA ha emitido el consejo para la práctica 2320-10

Alcance de la prueba

Naturaleza de la prueba

Contribución de los ITGCs a la evidencia de auditoría



Dependencias de TI

Cada vez que tenemos dependencias de TI, necesitamos considerar los ITGCs. Las deficiencias en los ITGCs pueden impactar nuestra habilidad de confiar en las dependencias de TI.

¿Que son las Dependencias de TI?

Cuando TI es utilizado para iniciar, autorizar, registrar, procesar o reportar transacciones o datos financieros para su inclusión en los estados financieros, ciertos datos, controles o reportes que utilizamos en nuestros procedimientos de prueba pueden depender de procedimientos de control automático o controles manuales dependientes de TI. Estos datos, controles o reportes representarán dependencias de TI.

Existen 5 tipos de Dependencias de TI

Controles Automáticos

Diseñados dentro de un sistema para hacer cumplir reglas de negocio.

Cálculos

Procedimientos contables que son ejecutados por un sistema de TI en vez de una persona.

Reportes

Información rutinariamente generada por sistemas de TI y a menudo utilizada en la ejecución de controles automáticos y manuales, incluyendo revisiones de desempeño del negocio, o como documentos fuente para realizar pruebas sustantivas.



Interfaces

Lógica programada que transfiere datos desde un sistema hacia otro.

Segregación de Funciones y Accesos Restringidos (Seguridad)

La seguridad, incluyendo la segregación de funciones hace posible que un sistema de TI restrinja el acceso a la información e identifique cualquier falta de separación de roles y responsabilidades que podría dejar a un empleado perpetrar y cometer errores o fraude, o que los errores en los procesos no sean detectados.

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Dependencias de TI

Identificar dependencias de TI es un asunto de juicio profesional que necesitamos aplicar basados en la manera en que los sistemas de TI interactúan con las líneas del estado financiero en alcance de nuestra revisión.

¿Son dependencias de TI?

1. Pregunta: Un cliente utiliza un sistema de payroll que funciona separado de su sistema de reporte financiero. Mensualmente, los datos del sistema de payroll son automáticamente registrados en el sistema de reporte financiero utilizando un proceso llamado interface. No existe intervención humana - ambos sistemas están automáticamente configurados para trabajar de esta manera. ¿Es una dependencia de TI? (SI/NO)

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

1. Respuesta: SI. La interface automática es una lógica programada que transfiere datos de un sistema a otro, sin intervención humana. Esto representa una dependencia de TI.
2. Pregunta: Mensualmente, el responsable de tesorería obtiene los extractos bancarios del sistema de banca online. Basado en las transacciones registradas en el sistema de registro financiero, el responsable efectúa una reconciliación entre los extractos del banco y el libro de caja. La reconciliación no es efectuada en una computadora. ¿Es una dependencia de TI? (SI/NO)

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

2. Respuesta: NO. Este proceso de conciliación bancaria manual no es una dependencia de TI, el proceso no depende de ninguna aplicación financiera significativa de TI. Si bien los extractos bancarios son extraídos del ambiente online del banco, esto no representa una dependencia de TI, ya que el ambiente online del banco no es parte del sistema de reporte financiero de la entidad. Aún así es necesario evaluar la confiabilidad de la información provista por ese sistema.

3. Pregunta: Una entidad tiene un almacén donde resguarda ítems de inventario de alto valor. El acceso al almacén es restringido mediante control biométrico de huella digital. Si la huella digital de un empleado no está registrada en el sistema, no se le permite el acceso. ¿Es una dependencia de TI? (SI/NO)

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

3. Respuesta: NO. No es una dependencia de TI, ya que el sistema de control de acceso físico al almacén no influencia o afecta a los sistemas de reporte financiero.

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Objetivos del procesamiento de la información



- **Integridad:** Todas las operaciones son ingresadas y aceptadas **una vez y solo una vez** a los fines del procesamiento, y en el **período apropiado**. Los asientos son **identificados** y las excepciones son **abordadas y resueltas**.
- **Precisión:** Las operaciones son registradas por el **monto correcto** en la **cuenta apropiada** y en el período apropiado (el ingreso de la fecha era correcto).
- **Validez:** Se registran sólo las operaciones **autorizadas** que sucedieron realmente y están relacionadas con la organización.
- **Acceso restringido:** Los datos son **protegidos contra cambios no autorizados** y el acceso a los datos confidenciales y activos físicos está restringido apropiadamente al personal autorizado.

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Objetivos del procesamiento de la información

Controles que ayudan a abordar la Integridad:

- Totales de procesamiento por lotes (proceso Batch)
- Verificación de secuencialidad
- Coincidencia por computadora (computer matching)
- Comprobaciones uno a uno

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Objetivos del procesamiento de la información

Controles que ayudan a abordar la Precisión (exactitud):

- Verificaciones de dependencias
- Verificaciones de formato
- Comparación de datos previos
- Verificaciones de razonabilidad
- Precisión matemática
- Entrada pregrabada
- Verificaciones de existencia
- Comprobaciones de dígitos verificadores
- Verificación clave

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Objetivos del procesamiento de la información

Controles que ayudan a abordar la Validez:

- Autorización manual
- Autorización de seguridad de la aplicación
- Comprobaciones de validez programadas
- Comprobación uno a uno

3. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Objetivos del procesamiento de la información

Controles que ayudan a abordar el Acceso Restringido

- Seguridad de datos
- Reportes de excepciones
- Conciliaciones de archivos
- Verificación detallada de datos en archivo

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

1. Entender el proceso de inicio a fin identificando riesgos potenciales de error

2. Identificar controles clave y evaluar su diseño e implementación

3. Testeo de controles y consideración de otra evidencia que respalde su efectividad operativa

4. Identificar y responder a deficiencias de control

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

- En el caso de muestreo estadístico, los resultados pueden ser extrapolados al universo.
- En el caso de muestreo no estadístico a juicio del auditor, los resultados no podrías ser extrapolados al universo.



Es importante identificar el origen de las excepciones



Identificar controles alternativos que minimicen el riesgo



Considerar experiencias de auditorias anteriores



Mantener escepticismo profesional respecto al resultado

03. PRUEBAS DE CONTROLES MANUALES Y AUTOMÁTICOS

Consultas, comentarios....

TIPS....

- Cuanto más **difícil** sea ejecutar el control, más alto es su riesgo y más evidencia necesitamos.
- Cuanto más **conocimientos** son requeridos para ejecutar el control, más alto es su riesgo y más evidencia necesitamos.
- Cuanto más relevantes son las **consecuencias** de la falla del control (p.e.: riesgo de errores), más alto es su riesgo y más evidencia necesitamos.

4

Conclusiones

3. CONCLUSIONES



La Unidad de Auditoría Interna será **responsable de la evaluación** del diseño, alcance y funcionamiento del Sistema de Control Interno, por lo cual, la Unidad debe evaluar por lo menos una vez al año el Sistema de Control interno de la Sociedad

Conforme lo establecen las Normas que regulan el trabajo de los Auditores Internos, es importante que para el testeo de controles automáticos y manuales se deje documentado el entendimiento y la descripción del control a ser verificado.

No te quedes solo con el resultado de las excepciones en las pruebas de controles, investiga el origen de la misma, puede existir una puerta abierta para que se materialice el riesgo.

Cuanto más relevantes son las consecuencias de la falla del control (p.e.: riesgo de errores), más alto es su riesgo y más evidencia necesitamos.

“Un hombre no mide su altura en los momentos de confort, sino en los de cambio y controversia...”

Martin Luther King

Pasaje Villegas, Edificio Ana María Piso 1, 2 y 3,
San Jorge, La Paz, Bolivia
+5 91 2408181

www.pwc.com/bo

PwC Bolivia



Valuación de activos financieros de acuerdo a la metodología ASFI

Programa de Capacitación - ABAV
FY2020



Agenda

- Motivación
- Marco normativo
- Metodología de valoración
 - Fuentes de información
 - Valoración de valores de renta fija
 - Valoración de valores de renta mixta
 - Valoración de valores de renta variable
 - Valoración de valores emitidos en el extranjero
- Caso práctico

Motivación

1

Motivación

- 

1 Brindar las herramientas para entender la valuación de las inversiones en el mercado de valores.
- 

2 Lograr la interacción entre participantes y el facilitador a través de la participación constante de los participantes del curso.
- 

3 Transmitir la experiencia adquirida en la valuación de las inversiones.
- 

4 Aplicar un caso práctico.

Marco normativo

2

Marco normativo

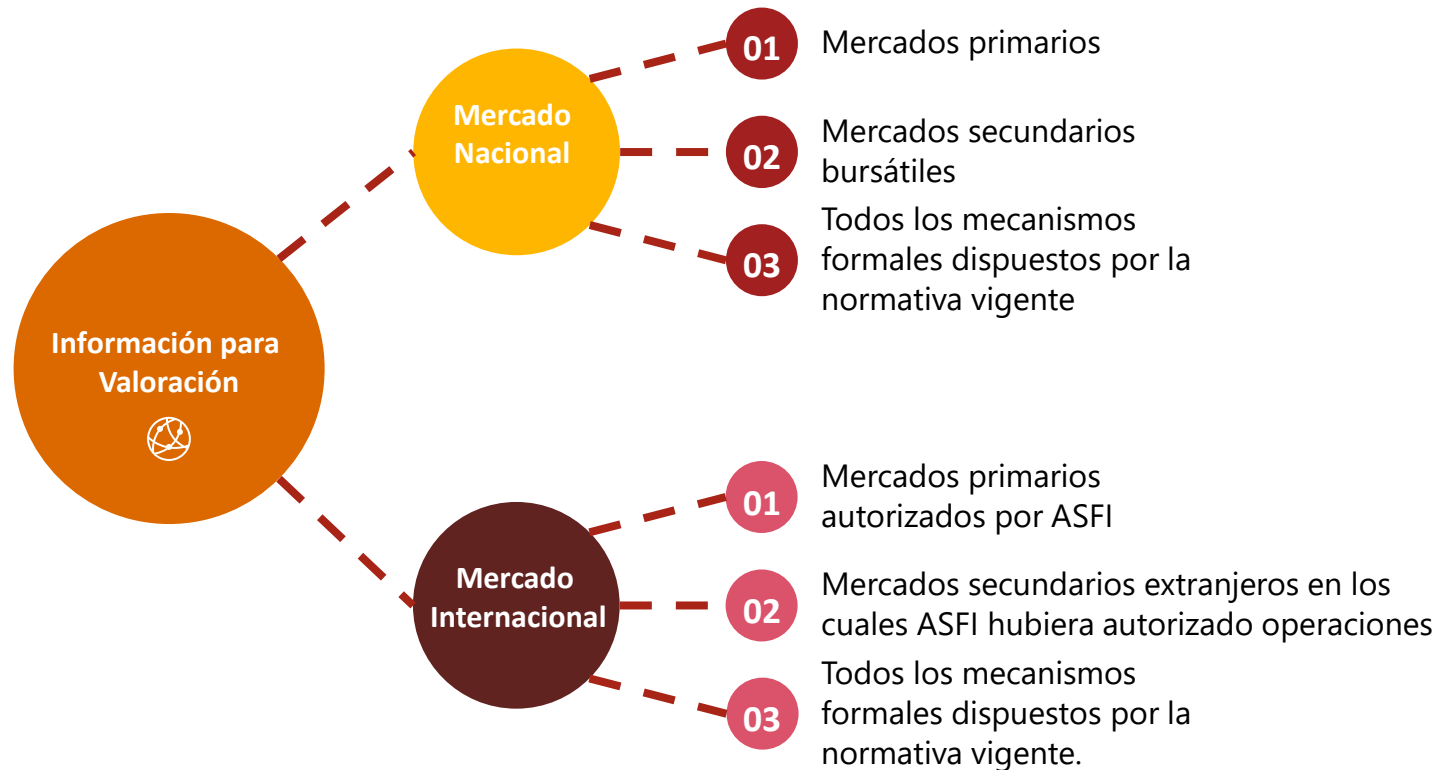
- Ley del mercado de valores
- Recopilación de normas para el mercado de valores
 - Metodología de valoración
 - Reglamento de control interno y auditores internos
- Resoluciones Administrativas emitidas por la Autoridad de Supervisión del Sistema Financiero, vigentes a la fecha referente a la Metodología de Valoración de Valores para las entidades supervisadas por la ASFI.

Metodología de valoración

3

Metodología de valoración

I. Fuentes de información para la valoración



Metodología de valoración (Cont.)

II. Valoración de valores de renta fija

a) Alternativas para la valoración:



Valoración a Tasa de Adquisición

En el evento que se adquiriera cualquier Valor



Valoración a Tasa de Mercado por Código de Valoración

Tasa de Rendimiento relevante será el promedio ponderado de las Tasas de Rendimiento de las transacciones del día



Valoración en caso de no existir transacciones en un día determinado

En el evento que en un día determinado no se transe ningún Valor de un mismo Código de Valoración



Valoración en caso de existir iteración entre rangos

En el caso de que en el día (t) se presente un hecho de mercado que afecte a uno o más valores de un mismo Código de Valoración

Metodología de valoración (Cont.)

II. Valoración de valores de renta fija (Cont.)

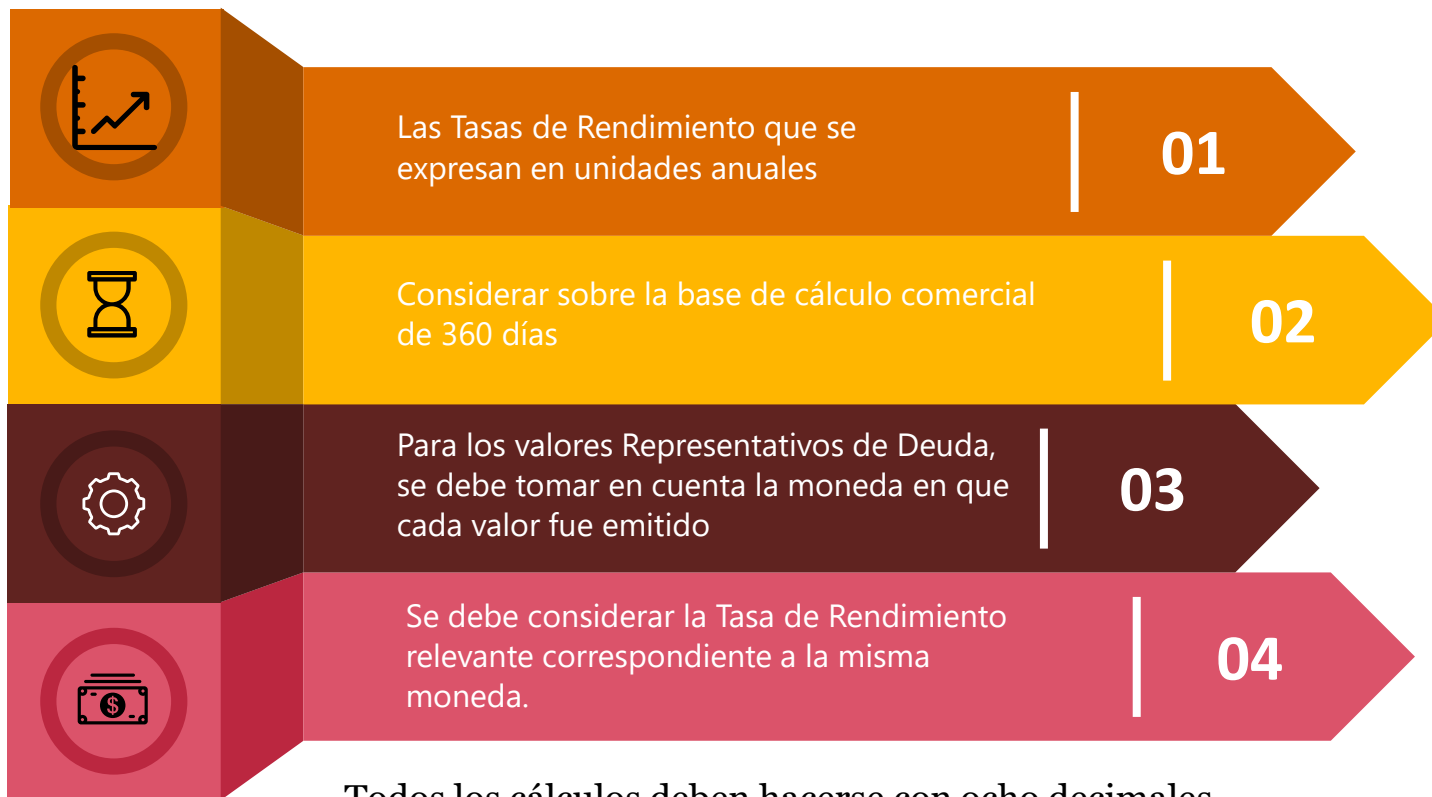
a) Alternativas para la valoración (Cont.):



Metodología de valoración (Cont.)

II. Valoración de valores de renta fija (Cont.)

b) Metodologías de cálculo



Todos los cálculos deben hacerse con ocho decimales, redondeando al último decimal

Metodología de valoración (Cont.)

II. Valoración de valores de renta fija (Cont.)

c) Procedimientos de cálculo para valores emitidos y negociados en mercados nacionales

i) *Valores emitidos y negociados a descuento o sin cupones.*

Tasa de Rendimiento Equivalente:

$$TRE = \frac{\left(1 + \frac{POR * TR}{360}\right)^{\frac{PEQ}{POR}} - 1}{PEQ} * 360$$

Metodología de valoración (Cont.)

II. Valoración de valores de renta fija (Cont.)

c) Procedimientos de cálculo para Valores emitidos y negociados en mercados nacionales (Cont.)

ii) Valores emitidos a rendimiento con cupones.

1. Monto de los cupones

$$VC_i = VN_i * (TR_e * \frac{Pl}{360})$$

2. Valores emitidos a rendimiento con plazos de cupones distintos y exactamente iguales

$$P_{it} = \sum_{c=1}^n \frac{F_c}{\prod_{a=1}^c \left(1 + TR * \frac{Pl_a}{360} \right)}$$

Metodología de valoración (Cont.)

II. Valoración de valores de renta fija (Cont.)

c) Procedimientos de cálculo para Valores emitidos y negociados en mercados nacionales (Cont.)

iii) Valores emitidos a tasa de rendimiento variable.

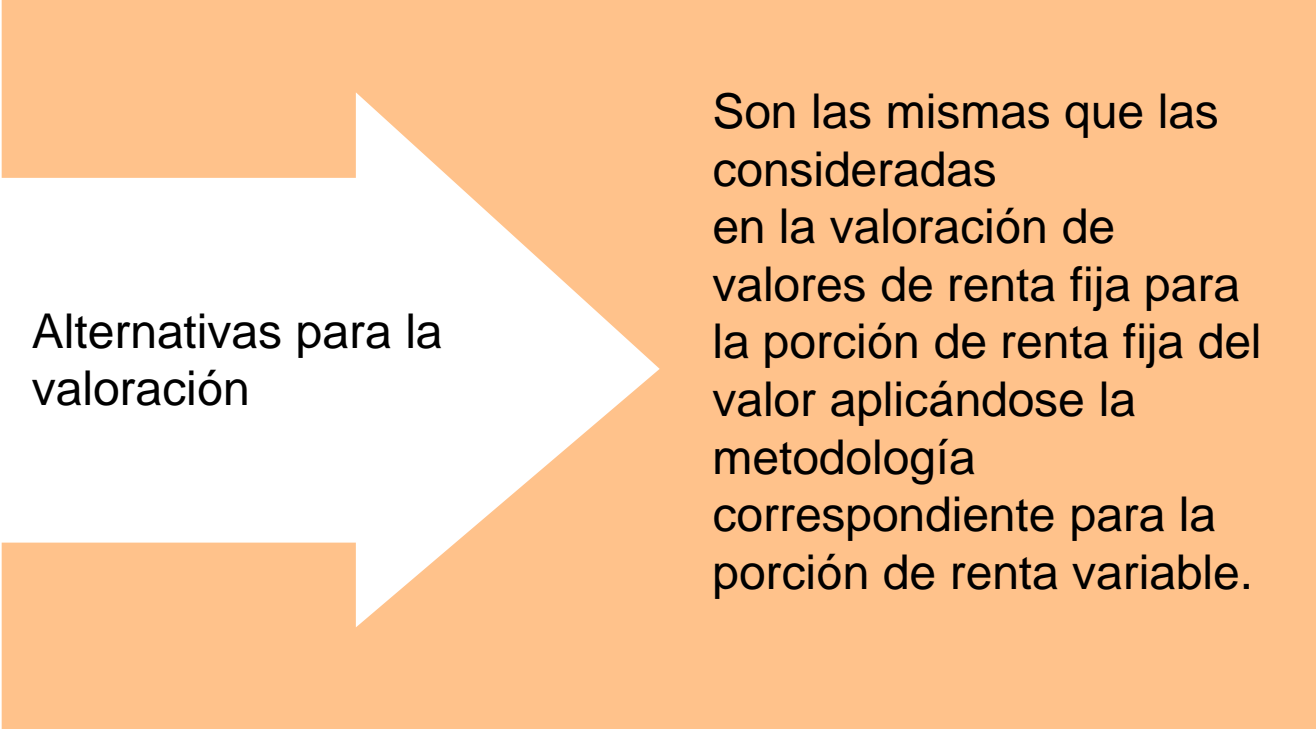
iv) Valores Emitidos Rendimientos con Prepagos del Principal (ó Capital).

- *Prepago de Valores directamente con el Emisor*
- *Prepago de Valores en Mercado Secundario*

Metodología de valoración (Cont.)

III. Valoración de valores de renta mixta

a) Alternativas para la valoración:



Alternativas para la valoración

Son las mismas que las consideradas en la valoración de valores de renta fija para la porción de renta fija del valor aplicándose la metodología correspondiente para la porción de renta variable.

Metodología de valoración (Cont.)

IV. Valoración de valores de renta variable

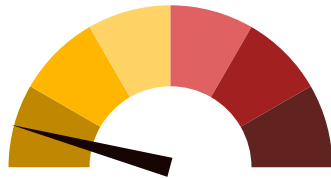
- a) Valoración de Valores de Renta Variable emitidos y negociados en mercados nacionales.



Metodología de valoración (Cont.)

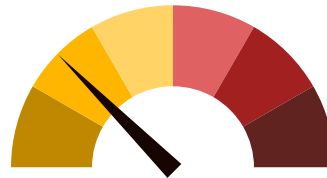
V. Valoración de valores emitidos en el extranjero

a) Fuentes de Información para inversiones en el extranjero



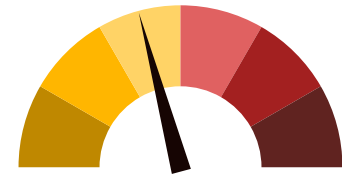
Bloomberg

Autorizada por ASFI



Reuters

Autorizada por ASFI



SIX Financial Information

Autorizada por ASFI

Los procedimientos y/o mecanismos para la obtención de los Precios o Tasas deberán ser establecidos y acordados entre las entidades supervisadas y la Bolsa de Valores o la Agencia de Información Financiera Internacional habilitada.

Metodología de valoración (Cont.)

V. Valoración de valores emitidos en el extranjero

b) Valoración de instrumentos de deuda extranjeros



Metodología de valoración (Cont.)

V. Valoración de valores emitidos en el extranjero

c) Valoración de instrumentos de renta variable

Acciones de empresas, cuotas de fondos de inversión cerrados y cuotas de fondos de inversión abiertos

Las acciones, cuotas de fondos de inversión cerrados y cuotas de fondos de inversión abiertos, se valorarán diariamente al último precio de cierre verificable y disponible a la fecha de cálculo, obtenido a partir de la Bolsa de Valores o de las Agencias de Información Financiera Internacional habilitadas.

Metodología de valoración (Cont.)

V. Valoración de valores emitidos en el extranjero

d) Valoración de Instrumentos Derivados y Estructurados

Instrumentos derivados (opciones, futuros, forwards) y estructurados

La valoración se realizará diariamente considerando el Precio de Cierre verificable y disponible proporcionado por la Bolsa de Valores u obtenido a partir de una Agencia de Información Financiera Internacional habilitada.

Metodología de valoración (Cont.)

V. Valoración de valores emitidos en el extranjero

c) Valoración en días no hábiles

Para fines de semana y ante la existencia de un feriado nacional o departamental en la ciudad sede de la Bolsa de Valores que informe los precios y tasas de los valores emitidos en el extranjero, las entidades supervisadas que cuenten con inversiones en el exterior deberán valorarlas utilizando los precios o tasas de mercado disponibles al último día hábil anterior al feriado o fin de semana, manteniendo los formatos y horarios de envío de información a ASFI.

Casos prácticos

4

Valores emitidos y negociados a descuento o sin cupones

Ejercicio N° 1

Se compra en el Mercado Primario un DPF con las siguientes condiciones:

DATOS:

Vli (Valor inicial o de compra) =	500.000
Tre (Tasa de rendimiento de la emisión)=	10%
Pl (Plazo en días) =	90

Se pide calcular:

- 1.- El valor final
- 2.- Tasa de rendimiento equivalente transcurrido un día
- 3.- Calcular el valor del DPF transcurrido un día

Valores emitidos a rendimiento con cupones

Ejercicio N° 2

Datos del DPF:

Fecha de Emisión =	02/08/2019
Fecha de Vencimiento =	27/07/2020

VN (Valor Nominal) =	500.000
TR (Tasa de rendimiento de emisión)=	10%
PI (Plazo en días) =	360

Cupón cada 90 días:

1°	31/10/2019
2°	29/01/2020
3°	28/04/2020
4°	27/07/2020

El 2/09/2019 se decide vender el Título.

Se pide calcular:

- 1.- El valor del cupón
- 2.- Precio del valor al 2/09/2019 fecha en la que se decide vender el Título
- 3.- El plazo económico a la fecha de la venta 02/09/2019

Gracias!!!

Esta publicación ha sido preparada para una orientación general acerca de asuntos de interés solamente, y no constituye asesoramiento profesional. Los receptores de la misma no deben actuar en base a la información contenida en esta publicación sin obtener asesoramiento independiente. No se efectúa manifestación ni se otorga garantía alguna (expresa o implícita) con respecto a la exactitud o integridad de la información contenida en esta publicación y, en la medida en que lo permite la ley, PwC, sus miembros, empleados y agentes no aceptan ni asumen ninguna responsabilidad, ni deber de cuidado por cualquier consecuencia de su accionar, o del accionar de terceros, o de negarse a actuar, confiando en la información contenida en esta publicación, o por ninguna decisión basada en la misma.

© 2020 PricewaterhouseCoopers S.R.L. Todos los derechos reservados. "PwC" se refiere a PricewaterhouseCoopers S.R.L., firma miembro de PricewaterhouseCoopers International Limited, cada firma miembro es una entidad legal separada.

Entendiendo y respondiendo a los riesgos de TI



Entendiendo y respondiendo a los riesgos de TI



A continuación se expone una visión general de los Controles Generales de Tecnología de la Información, su contribución a la evidencia de Auditoría y alguno de los elementos a considerar en el diseño e implementación de nuestra estrategia con relación a los Controles Generales de Tecnología de la Información.



Tipos de Controles

Controles a nivel transacción, controles a nivel de entidad, consideraciones a nivel de proceso y controles generales de tecnología de la información.

Existen diferentes tipos de controles implementados en los procesos y subprocesos del negocio. Es importante distinguir un control de otro, considerando el tipo de control cuando identificamos controles dentro de un proceso de negocio.



Consideraciones a nivel de proceso son actividades de control (ya sea a nivel transaccional o a nivel entidad) ejecutados a un nivel del proceso de negocio que necesita ser considerado cuando evaluamos la efectividad de los controles a nivel transaccional o controles que ocurren a nivel de la entidad dentro de un proceso de negocio. Esta relacionado con los siguientes tópicos:

- Controles sobre datos permanentes.
- Controles sobre herramientas computacionales a nivel de usuario final, como ser hojas electrónicas.
- Segregación de funciones
- Uso de organizaciones de servicio.
- Revisiones gerenciales de derechos de acceso a sistemas.
- Posteos del sistema (basadas en esquemas de cuentas contables pre-establecidos).

Controles a nivel de Entidad (ELCs)

son controles que típicamente operan a un nivel más alto que los controles transaccionales. Su propósito es prevenir, o detectar y corregir oportunamente errores materiales en procesos de negocio o en una o más aserciones a nivel de línea de estados financieros.

Ejemplos:

Políticas y procedimientos de recursos humanos.
Revisiones de desempeño del negocio.

Controles a nivel de Entidad Directos

Típicamente operan a un nivel más alto que el nivel de sub-proceso y cuando son ejecutados efectivamente, a un suficiente nivel de precisión, previenen o detectan y corrigen oportunamente errores materiales en procesos de negocio.

Ejemplo: Revisiones de desempeño del negocio.

Controles a nivel de Entidad Indirectos

No relacionados directamente con ningún proceso de negocio o línea del estado financiero o aserciones, consecuentemente, por si mismos no previenen o detectan y corrigen errores. Sin embargo, contribuyen a la efectividad de los controles.

Ejemplo: Código de Conducta.

Controles transaccionales

Son actividades de control sobre el inicio, registro, procesamiento o reporte de transacciones individuales.

Los controles transaccionales pueden ser de naturaleza detectiva o preventiva. Pueden ser manuales, automáticos o manuales dependientes de TI.

Ejemplos: aprobación de órdenes de compra.

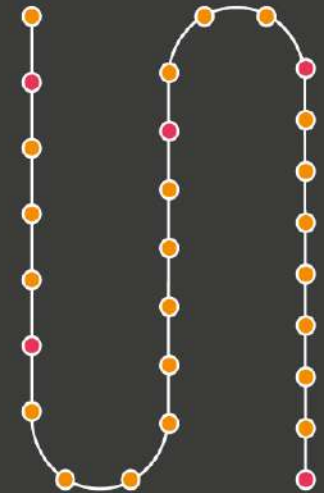


Controles Generales de TI (ITGCs)

Son controles que sirven para administrar y controlar las actividades de tecnología de información y el ambiente tecnológico, se relacionan con muchas aplicaciones y soportan el funcionamiento efectivo de los controles de aplicación ayudando a verificar la operación continua de los sistemas de información. Los ITGCs cubren las siguientes áreas: Desarrollo de Programas, Cambios a Programas, Accesos a programas y Datos, Operaciones Computarizadas.

Tipos de Procesos de Negocio

Enero



Diciembre

Procesos de negocio periódicos

Incluyen actividades de control sobre el inicio, registro, procesamiento y reporte de una baja cantidad de transacciones, incluyendo transacciones de una sola vez o transacciones no frecuentes. Por ejemplo: activos intangibles.

Procesos de negocio transaccionales

Incluyen actividades de control sobre el inicio, registro, procesamiento y reporte de un alto número y diferentes tipos de transacciones rutinarias a través del periodo. Por ejemplo procesos de negocio de compras y pagos, ventas y cuentas por cobrar.

Entendiendo y respondiendo a los riesgos de TI



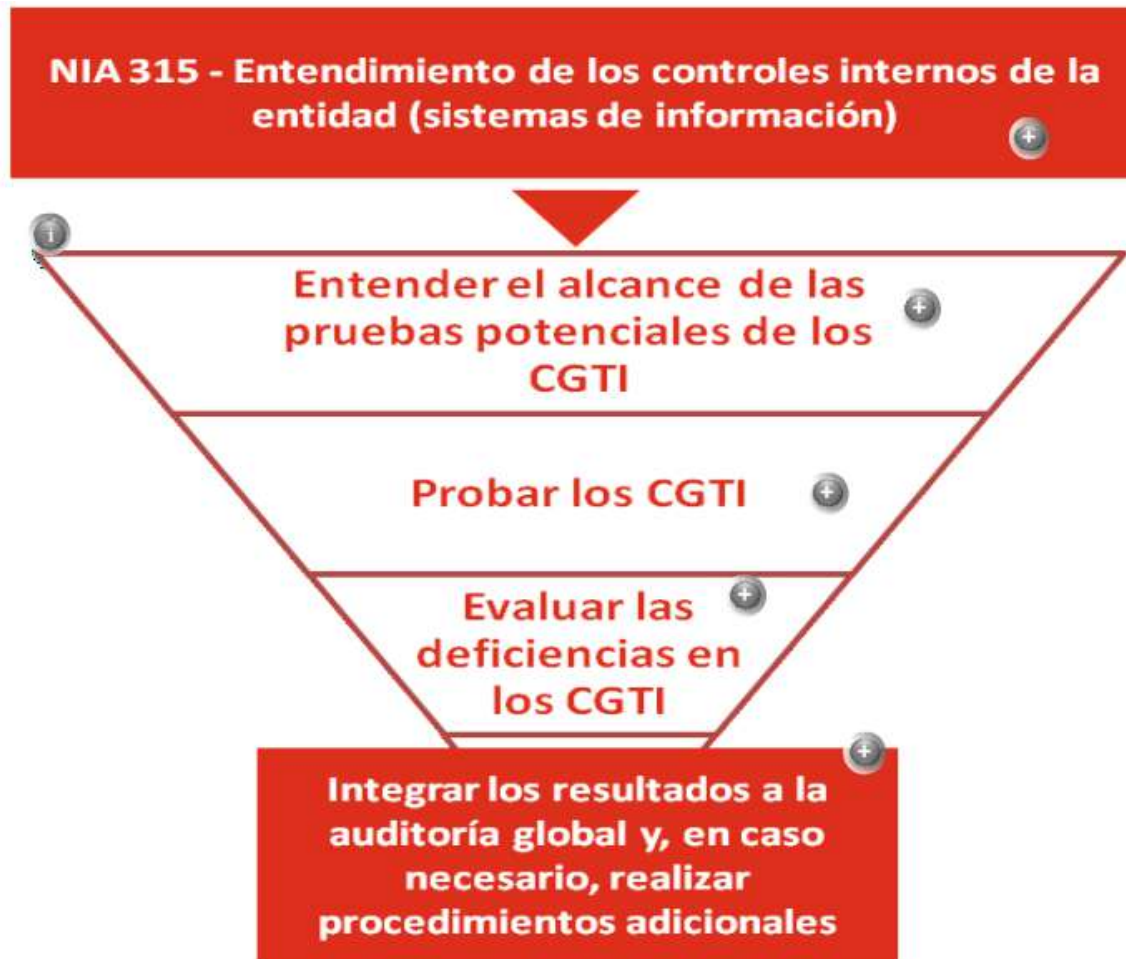
Los estados financieros se basan en información financiera que frecuentemente es generada, registrada, procesada y reportada por sistemas de TI.

Existen varios tipos de controles que nos ayudan a asegurarnos de que los sistemas de TI estén funcionando de manera efectiva. Los llamados ITGCs son uno de estos controles. La NIA 315 define los ITGC como "políticas y procedimientos comunes a muchas aplicaciones que respaldan el funcionamiento efectivo de los controles de aplicación".

Adicionalmente se mostrará algunos factores que se deben considerar a la hora de diseñar e implementar el enfoque de pruebas de los ITGCs.

Entendiendo y respondiendo a los riesgos de TI

Proceso de principio a fin para probar los ITGCs:



Entendiendo y respondiendo a los riesgos de TI



Módulo 2

La NIA 315 requiere que el auditor obtenga un entendimiento de los sistemas de información, incluyendo los procesos del negocio relacionados, que son relevantes para la información financiera.

En este módulo aprenderá más acerca de cómo este requerimiento aplica a los CGTI.

Entendiendo y respondiendo a los riesgos de TI

Entendimiento de sistemas de información

El primer paso, y a menudo el más importante, para determinar el alcance del trabajo de auditoría a realizar con los CGTI es obtener un entendimiento de los [sistemas de información de la entidad](#), incluyendo los procesos del negocio relacionados, que son relevantes para la información financiera.

Independientemente del tamaño del cliente o de si decide probar los CGTI o no, bajo la NIA 315 "Identificación y evaluación de los riesgos de errores significativos mediante el entendimiento de la entidad y su entorno", estará obligado a obtener dicho entendimiento.

Deberá entender, entre otros:

- Las clases de transacciones que son significativas para los estados financieros
- Los procedimientos, tanto automatizados como manuales, que generan, procesan y transfieren dichas transacciones al libro mayor
- Cómo los sistemas de información captan eventos y condiciones (excluyendo las transacciones)
- La visión de la gerencia de la función de TI (historial de errores o excepciones significativas)
- Cómo la entidad ha respondido ante los riesgos de TI y
- Las FSLI que están dentro del alcance y cómo deberán ser mapeadas a los sistemas.

Information & Communication		Go to Secondary tab
<input type="checkbox"/> Inquired of entity personnel on the understanding and evaluation of design effectiveness of the control relevant to the audit.		Document details, scope and date of inquiry
Controls relevant to the audit	Understanding and evaluation of design effectiveness	Evidence of control implementation
Complexity of IT systems Determine if the entity's IT system is complex or non-complex and if non-complex, determine if the entity's IT system is an off-the-shelf package.	Determined that IT system is complex and required involvement of SPA specialists documented in the EGA "Team mobilization". This determination is based on (checked those that apply): <ul style="list-style-type: none"> <input type="checkbox"/> System has automated complex calculations (e.g., calculation of insurance premium). <input type="checkbox"/> System is an older technology that is no longer or poorly supported by vendors. <input type="checkbox"/> System is a new and emerging technology not yet widely used. <input type="checkbox"/> System is entity-developed or a highly modified off-the-shelf software. <input type="checkbox"/> System is an Enterprise Resource Planning (ERP) system. <input type="checkbox"/> There are extensive customized interfaces between systems. <input type="checkbox"/> System processes a high volume of transactions (e.g., bank and retail operations). <input type="checkbox"/> System processes for a complex or sophisticated business entity (e.g., multinational operations). <input type="checkbox"/> System is part of a complex information technology infrastructure (e.g., multiple sites, multiple systems). <input type="checkbox"/> <i>Other (specify)</i> <p style="text-align: center;">OR</p> <input type="checkbox"/> Determined that IT system is non-complex, optional involvement of SPA specialists documented in the EGA "Team mobilization", and (document rationale) <ul style="list-style-type: none"> <input type="checkbox"/> Determined that the IT system is an off-the-shelf package. (document details or link to the "Off the shelf" packages questionnaire" available on Compliance Manager) <input type="checkbox"/> Determined that the IT system is not an off-the-shelf package. (document details or link to the "Off the shelf" packages questionnaire" available on Compliance Manager) <p style="text-align: center;">OR</p> <input type="checkbox"/> Assessment of IT system complexity performed separately in a questionnaire. (provide link)	

Entendiendo y respondiendo a los riesgos de TI

¿Dónde estoy?

Ahora sabe que la NIA 315 requiere que obtenga un entendimiento de los sistemas de información de su cliente.

Este conocimiento le servirá como base para completar el siguiente módulo: Entender el alcance de las pruebas potenciales de los CGTI.



Entendiendo y respondiendo a los riesgos de TI



Módulo 3

Introducción - En este módulo aprenderá acerca de los factores que debe considerar a la hora de determinar el alcance de las pruebas potenciales a los CGTI.

Entendiendo y respondiendo a los riesgos de TI

Determinar el alcance de los CGTI - Controles de sistemas y de aplicación

Para poder determinar adecuadamente el alcance de las pruebas a los CGTI, debe identificar los CGTI que son relevantes para la auditoría. Una vez que obtenga un entendimiento de los sistemas de información del cliente, debe determinar qué controles de sistemas y de aplicación subyacentes desea probar.

Abajo encontrará definiciones y ejemplos de varios controles de aplicación.

 *Click en cada procedimiento automatizado para ver la definición y un ejemplo*

Reporte

Cálculo

Controles automatizados
(Ej. Cotejo Triple)

La seguridad
(incluyendo la segregación de funciones)

Interfaces

Entendiendo y respondiendo a los riesgos de TI

Determinar el alcance de los CGTI - Controles de sistemas y de aplicación

Para poder determinar adecuadamente el alcance de las pruebas a los CGTI, debe identificar los CGTI que son relevantes para la auditoría. Una vez que obtenga un entendimiento de los sistemas de información del cliente, debe determinar qué controles de sistemas y de aplicación subyacentes desea probar.

Abajo encontrará definiciones y ejemplos de varios controles de aplicación.

 Click en cada procedimiento automatizado para ver la definición y un ejemplo

Reporte

Definición: Los reportes generados por el sistema pueden ser utilizados para la ejecución de un control manual, incluyendo revisiones de desempeño del negocio, o como documentos fuente para pruebas de auditoría sustantivas.

Ejemplo: Algunos ejemplos de reportes generados por el sistema que pueden ser utilizados son un balance de comprobación, un reporte de antigüedad de cuentas por cobrar, un reporte de transacciones rechazadas, etc.

Consulte "Ejemplos de reportes generados por el sistema y técnicas de pruebas" en la pestaña de recursos para ver ejemplos de técnicas de pruebas que podrían ser utilizadas para obtener evidencia de auditoría sobre la confiabilidad de los reportes del sistema.

Interfaces

la seguridad
incluyendo la
gregación de
(funciones)

Entendiendo y respondiendo a los riesgos de TI

Determinar el alcance de los CGTI - Controles de sistemas y de aplicación

Para poder determinar adecuadamente el alcance de las pruebas a los CGTI, debe identificar los CGTI que son relevantes para la auditoría. Una vez que obtenga un entendimiento de los sistemas de información del cliente, debe determinar qué controles de sistemas y de aplicación subyacentes desea probar.

Abajo encontrará definiciones y ejemplos de varios controles de aplicación.

 *Click en cada procedimiento automatizado para ver la definición y un ejemplo*

Reporte

Controles
automatizados
(Ej. Cotejo
Triple)

Interfaces

Cálculo

Definición: Los cálculos son procedimientos de contabilidad realizados por un sistema de TI en vez de una persona.

X

Ejemplo: El sistema aplicará una la fórmula de depreciación por línea recta para calcular la depreciación de un activo (el costo del activo menos el valor residual del activo al término de su vida útil dividido entre la vida útil del activo).

Entendiendo y respondiendo a los riesgos de TI

Determinar el alcance de los CGTI - Controles de sistemas y de aplicación

Para poder determinar adecuadamente el alcance de las pruebas a los CGTI, debe identificar los CGTI que son relevantes para la auditoría. Una vez que obtenga un entendimiento de los sistemas de información del cliente, debe determinar qué controles de sistemas y de aplicación subyacentes desea probar.

Abajo encontrará definiciones y ejemplos de varios controles de aplicación.

 *Click en cada procedimiento automatizado para ver la definición y un ejemplo*



Definición: Los controles automatizados se incluyen dentro de un sistema para garantizar el cumplimiento de las reglas del negocio. X

Ejemplo: Muchos sistemas de TI incluyen verificaciones de formato (p. ej. fecha o número), verificaciones de existencia (p. ej. que el número del cliente aparezca en el archivo maestro del cliente) o verificaciones de razonabilidad (p. ej. monto máximo del pago) cuando se registra una transacción.



Entendiendo y respondiendo a los riesgos de TI

Determinar el alcance de los CGTI - Controles de sistemas y de aplicación

Para poder determinar adecuadamente el alcance de las pruebas a los CGTI, debe identificar los CGTI que son relevantes para la auditoría. Una vez que obtenga un entendimiento de los sistemas de información del cliente, debe determinar qué controles de sistemas y de aplicación subyacentes desea probar.

Abajo encontrará definiciones y ejemplos de varios controles de aplicación.

 *Click en cada procedimiento automatizado para ver la definición y un ejemplo*

Reporte

Controles automatizados
(Ej. Cotejo Triple)

Interfaces

Definición: La seguridad, incluyendo la segregación de funciones, es habilitada por el sistema de TI para restringir el acceso a la información y garantizar una adecuada segregación de roles y responsabilidades para así evitar que un empleado cometa u oculte errores o fraudes.

Ejemplo: Al usuario se le pide una contraseña para acceder al sistema de TI.

La seguridad
(incluyendo la
segregación de
funciones)

Entendiendo y respondiendo a los riesgos de TI

Determinar el alcance de los CGTI - Controles de sistemas y de aplicación

Para poder determinar adecuadamente el alcance de las pruebas a los CGTI, debe identificar los CGTI que son relevantes para la auditoría. Una vez que obtenga un entendimiento de los sistemas de información del cliente, debe determinar qué controles de sistemas y de aplicación subyacentes desea probar.

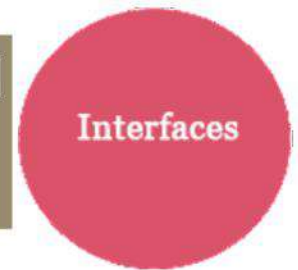
Abajo encontrará definiciones y ejemplos de varios controles de aplicación.

 *Click en cada procedimiento automatizado para ver la definición y un ejemplo*



Definición: Las interfaces son lógicas programadas que transfieren datos de un sistema de TI a otro.

Ejemplo: Se podría programar una interfaz para transferir datos del auxiliar de nómina al libro mayor.

An orange circle containing the text "La seguridad (incluyendo la segregación de funciones)" in white text.

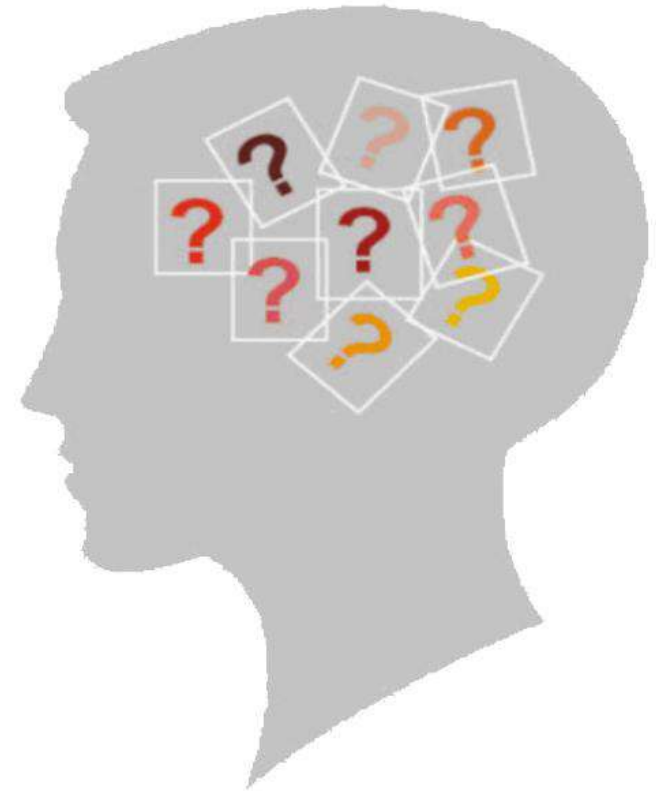
Entendiendo y respondiendo a los riesgos de TI

¿Cuándo debemos probar los CGTI?

Recuerde que los CGTI nos ayudan indirectamente a establecer la confiabilidad de los controles de aplicación. El equipo de auditoría deberá determinar si probar los CGTI resulta eficiente y efectivo.

Algunos factores que debe considerar a la hora de tomar una decisión son:

- Si espera que los CGTI sean efectivos. Si piensa que los CGTI no serán efectivos, resultaría ineficiente probarlos.
- El número de controles de aplicación y el riesgo asociado con dichos controles; por ejemplo, el impacto potencial sobre los estados financieros si algo falla en el sistema. Cuanto mayor sea el número de controles de aplicación con un alto riesgo asociado, mayor será la probabilidad de que los equipos prueben los CGTI si piensan que serán efectivos (y vice versa). Por ejemplo, si una aplicación genera muy pocos reportes, podría resultar más eficiente probar la integridad y exactitud de los mismos reportes en vez de probar los CGTI. Encontrará un modelo de un plan de pruebas para sistemas de TI no complejos en la pestaña de recursos bajo "Probar los CGTI – Sistemas no complejos".



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Determinar el alcance

? ¿En qué situación estaría MENOS inclinado a probar los CGTI?

- a) Un sistema que genera un reporte de los estados financieros todos los meses, utilizado por la gerencia para sus revisiones de desempeño del negocio.
- b) Un sistema de registro de materia prima, el cual genera un listado de inventarios que serán utilizados en el almacén. El sistema no tiene interfaz con el libro mayor y los datos son revisados manualmente.
- c) Un sistema de ventas que registra los datos de las transacciones de venta en el libro mayor.

Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Determinar el alcance

 ¿En qué situación estaría MENOS inclinado a probar los CGTI?

- a) Un sistema que genera un reporte de los estados financieros todos los meses, utilizado por la gerencia para sus revisiones de desempeño del negocio.
- b) Un sistema de registro de materia prima, el cual genera un listado de inventarios que serán utilizados en el almacén. El sistema no tiene interfaz con el libro mayor y los datos son revisados manualmente.
- c) Un sistema de ventas que registra los datos de las transacciones de venta en el libro mayor.

Entendiendo y respondiendo a los riesgos de TI

¿Dónde estoy?

En este módulo aprendió que después de obtener un entendimiento de los sistemas de información de la entidad que son relevantes para la información financiera, debe identificar los controles de sistemas y de aplicación subyacentes que usará para obtener evidencia de auditoría y considerar si probar los CGTI representa una manera eficiente de obtener dicha evidencia.

En el próximo módulo conocerá algunos de los factores clave que debe considerar para desarrollar su estrategia de pruebas.



Entendiendo y respondiendo a los riesgos de TI



Módulo 4

En este módulo aprenderá acerca de los factores que debe considerar para desarrollar una estrategia de pruebas para los CGTI.

Entendiendo y respondiendo a los riesgos de TI

Complejidad del sistema

El primer factor que debe considerar cuando esté desarrollando una estrategia de pruebas para los CGTI es la complejidad del sistema.

Los equipos de auditoría deben clasificar los sistemas clave del cliente en:

- complejos o
- no complejos

Encontrará un modelo de un plan de pruebas para sistemas de TI no complejos en la pestaña de recursos bajo "Probar los CGTI – Sistemas no complejos".

 *Click en cada burbuja para ver ejemplos de clasificación*

[Mas Información](#)

Sistemas de TI
complejos (p. ej.
SAP, Oracle)

Sistemas de TI no
complejos (p. ej.
QuickBooks, CODA)

Entendiendo y respondiendo a los riesgos de TI

Complejidad del sistema

El primer factor que debe considerar cuando esté desarrollando una estrategia de pruebas para los CGTI es la complejidad del sistema.

Los equipos de auditoría deben clasificar los sistemas clave del cliente en:

- complejos o
- no complejos

Encontrará un modelo de un plan de pruebas para sistemas de TI no complejos en la pestaña de recursos bajo "Probar los CGTI – Sistemas no complejos".

 *Click en cada burbuja para ver ejemplos de clasificación*

Sistemas de TI complejos (p. ej. SAP, Oracle)

Sistemas de TI no complejos (p. ej. QuickBooks, CODA)

Más Información

Sistemas de TI complejos (p. ej. SAP, Oracle)

Cualquiera de los siguientes factores podría ser un indicador de la existencia de sistemas complejos de TI:

- Sistemas con cálculos automatizados complejos (p. ej. cálculo de primas de seguro, cálculo de costos de producción).
- Tecnología vieja con poco o ningún servicio de soporte de proveedores.
- Tecnología nueva o emergente que aún no es de uso masivo.
- Software desarrollado por la entidad o software comercial extensamente modificado.
- Sistemas de planificación de recursos empresariales (ERP) (p. ej. SAP, Oracle, JD Edwards).

Continuación...

Entendiendo y respondiendo a los riesgos de TI

Complejidad del sistema

El primer factor que debe considerar cuando esté desarrollando una estrategia de pruebas para los CGTI es la complejidad del sistema.

Los equipos de auditoría deben clasificar los sistemas clave del cliente en:

- complejos o
- no complejos

Encontrará un modelo de un plan de pruebas para sistemas de TI no complejos en la pestaña de recursos bajo "Probar los CGTI – Sistemas no complejos".

 *Click en cada burbuja para ver ejemplos de clasificación*

Sistemas de TI
complejos (p. ej.
SAP, Oracle)

Sistemas de TI no
complejos (p. ej.
QuickBooks, CODA)

Más Información

Sistemas de TI complejos (p. ej. SAP, Oracle)

- Interfaces entre sistemas altamente personalizadas.
- Sistemas que procesan un gran volumen de transacciones (p. ej. operaciones bancarias y de minoristas).
- Sistemas de empresas complejas o sofisticadas (p. ej. operaciones multinacionales).
- Infraestructura de TI compleja (p. ej. sitios múltiples, sistemas múltiples).

Atras...

Entendiendo y respondiendo a los riesgos de TI

Complejidad del sistema

El primer factor que debe considerar cuando esté desarrollando una estrategia de pruebas para los CGTI es la complejidad del sistema.

Los equipos de auditoría deben clasificar los sistemas clave del cliente en:

- complejos o
- no complejos

Encontrará un modelo de un plan de pruebas para sistemas de TI no complejos en la pestaña de recursos bajo "Probar los CGTI – Sistemas no complejos".

 *Click en cada burbuja para ver ejemplos de clasificación*

Sistemas de TI complejos (p. ej. SAP, Oracle)

Sistemas de TI no complejos (p. ej. QuickBooks, CODA)

Más Información

Sistemas de TI no complejos (p. ej. QuickBooks, CODA)

Los sistemas de TI podrían ser no complejos si se cumplen todos los siguientes factores:

- Software comercial de uso masivo con buen servicio de soporte de proveedores.
- La personalización o configuración de los sistemas es relativamente menor (p. ej. configuración de reportes simples, personalización de la plantilla para facturas de venta) o no se puede realizar.
- Ausencia de o pocas recuperaciones de datos en las bases de datos subyacentes. Muy pocos usuarios de TI tienen acceso directo a los registros de las bases de datos.
- Estabilidad (es decir, ausencia de actualizaciones mayores o nuevas implementaciones).

Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.




Click a las imágenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 Click a las imágenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía cuenta con un solo sistema de aplicaciones para procesar todas las transacciones clave del negocio. La compañía no tiene acceso al código fuente. No existe un departamento de Tecnología y todo el soporte de TI se obtiene directamente del proveedor. No se han hecho requerimientos de soporte de TI en los últimos cinco años.

Complejo

No Complejo


 Click en la opción apropiada para clasificar el sistema



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 Click a las imágenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía cuenta con un solo sistema de aplicaciones para procesar todas las transacciones clave del negocio. La compañía no tiene acceso al código fuente. No existe un departamento de Tecnología y todo el soporte de TI se obtiene directamente del proveedor. No se han hecho requerimientos de soporte de TI en los últimos cinco años.

Complejo

No Complejo

¡Es correcto! Este es un sistema no complejo.

 Click en la opción apropiada para clasificar el sistema



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 Click a las imagenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía usa un sistema SAP soportado por su casa matriz. Cualquier solicitud para cambio de programas o de accesos es remitida a la casa matriz para su procesamiento y aprobación.

Complejo

No Complejo


 Click en la opción apropiada para clasificar el sistema



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 Click a las imágenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía usa un sistema SAP soportado por su casa matriz. Cualquier solicitud para cambio de programas o de accesos es remitida a la casa matriz para su procesamiento y aprobación.

Complejo

¡Es correcto! Este es un sistema complejo.

No Complejo

 Click en la opción apropiada para clasificar el sistema



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 Click a las imágenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía familiar genera transacciones de bajo volumen pero de grandes montos en dólares. La compañía utiliza un sistema viejo de TI altamente personalizado que ya no cuenta con servicio de soporte del proveedor. El acceso al sistema es autorizado por el presidente o gerente ejecutivo. Cualquier persona que desee acceder al sistema debe tener una identificación de usuario independiente. Dos personas tienen permisos de superusuario.

Complejo

No Complejo


 Click en la opción apropiada para clasificar el sistema



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 Click a las imagenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía familiar genera transacciones de bajo volumen pero de grandes montos en dólares. La compañía utiliza un sistema viejo de TI altamente personalizado que ya no cuenta con servicio de soporte del proveedor. El acceso al sistema es autorizado por el presidente o gerente ejecutivo. Cualquier persona que desee acceder al sistema debe tener una identificación de usuario independiente. Dos personas tienen permisos de superusuario.

Complejo

¡Es correcto! Este es un sistema complejo.

No Complejo

 Click en la opción apropiada para clasificar el sistema



Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.



Click a las imágenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente



Una compañía utiliza el software comercial QuickBooks para procesar sus transacciones clave. En QuickBooks las transacciones de ventas son registradas y facturadas en una aplicación de ventas basada en Internet con servicio de soporte del proveedor.



Click en la opción apropiada para clasificar el sistema

Complejo

No Complejo

Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Clasificar los sistemas

Ahora apliquemos estos conocimientos sobre los sistemas.

 *Click a las imagenes para leer la descripción que te ayudara a clasificarlas en el sistema correspondiente*



Una compañía utiliza el software comercial QuickBooks para procesar sus transacciones clave. En QuickBooks las transacciones de ventas son registradas y facturadas en una aplicación de ventas basada en Internet con servicio de soporte del proveedor.

 *Click en la opción apropiada para clasificar el sistema*

Complejo

¡Es correcto! Este es un sistema complejo.

No Complejo

Entendiendo y respondiendo a los riesgos de TI

Evaluación de riesgos de TI

El próximo factor que debe considerar cuando esté desarrollando una estrategia de pruebas es el riesgo. Identificar los riesgos le ayudará a incrementar la calidad y eficiencia de la auditoría.

La NIA 315.A63 incluye ejemplos de riesgos específicos relacionados con TI. El diagrama que se muestra abajo incluye ejemplos de riesgos estándar (con base en la NIA 315) que generalmente consideramos cuando analizamos los cuatro dominios de TI. Consulte el folleto "Probar los CGTI – Evaluación de riesgos de TI" en la pestaña de recursos para ver los factores clave a considerar para evaluar los riesgos de TI más relevantes.



 Click en los 4 dominios de TI para encontrar los riesgos cubiertos

Más Información

Entendiendo y respondiendo a los riesgos de TI

Evaluación de riesgos de TI

El próximo factor que debe considerar cuando esté desarrollando una estrategia de pruebas es el riesgo. Identificar los riesgos le ayudará a incrementar la calidad y eficiencia de la auditoría.

La NIA 315.A63 incluye ejemplos de riesgos específicos relacionados con TI. El diagrama que se muestra abajo incluye ejemplos de riesgos estándar (con base en la NIA 315) que generalmente consideramos cuando analizamos los cuatro dominios de TI. Consulte el folleto "Probar los CGTI – Evaluación de riesgos de TI" en la pestaña de recursos para ver los factores clave a considerar para evaluar los riesgos de TI más relevantes.



Click en los 4 dominios de TI para encontrar los riesgos cubiertos

Más Información

Acceso a programas y datos

- Usuarios de las aplicaciones del negocio que evaden las autorizaciones impuestas por el sistema o los controles de segregación de funciones.
- Personal de Tecnología u otros administradores de acceso a usuarios que evaden los controles normales de acceso o de segregación de funciones.
- Cambios directos inapropiados a registros de transacciones subyacentes o archivos maestro.

Entendiendo y respondiendo a los riesgos de TI

Evaluación de riesgos de TI

El próximo factor que debe considerar cuando esté desarrollando una estrategia de pruebas es el riesgo. Identificar los riesgos le ayudará a incrementar la calidad y eficiencia de la auditoría.

La NIA 315.A63 incluye ejemplos de riesgos específicos relacionados con TI. El diagrama que se muestra abajo incluye ejemplos de riesgos estándar (con base en la NIA 315) que generalmente consideramos cuando analizamos los cuatro dominios de TI. Consulte el folleto "Probar los CGTI – Evaluación de riesgos de TI" en la pestaña de recursos para ver los factores clave a considerar para evaluar los riesgos de TI más relevantes.



 [Click en los 4 dominios de TI para encontrar los riesgos cubiertos](#)

Mas Información

Cambios a programas

- No hacer los cambios necesarios a sistemas o programas.
- Cambios que introducen errores en las aplicaciones.
- Cambios directos no autorizados a códigos de aplicación, evadiendo así el control de cambios.
- Cambios directos no autorizados a la configuración de aplicaciones, evadiendo así el control de cambios.
- Actualizaciones al ambiente de TI que impiden el correcto funcionamiento de las aplicaciones.

Entendiendo y respondiendo a los riesgos de TI

Evaluación de riesgos de TI

El próximo factor que debe considerar cuando esté desarrollando una estrategia de pruebas es el riesgo. Identificar los riesgos le ayudará a incrementar la calidad y eficiencia de la auditoría.

La NIA 315.A63 incluye ejemplos de riesgos específicos relacionados con TI. El diagrama que se muestra abajo incluye ejemplos de riesgos estándar (con base en la NIA 315) que generalmente consideramos cuando analizamos los cuatro dominios de TI. Consulte el folleto "Probar los CGTI – Evaluación de riesgos de TI" en la pestaña de recursos para ver los factores clave a considerar para evaluar los riesgos de TI más relevantes.



 [Click en los 4 dominios de TI para encontrar los riesgos cubiertos](#)

Más Información

Operaciones computarizadas

- Intervención manual inapropiada o fallas en el procesamiento por lotes.
- Fallas del sistema que causan pérdida de los registros de transacciones o incapacidad de acceso.

Entendiendo y respondiendo a los riesgos de TI

Evaluación de riesgos de TI

El próximo factor que debe considerar cuando esté desarrollando una estrategia de pruebas es el riesgo. Identificar los riesgos le ayudará a incrementar la calidad y eficiencia de la auditoría.

La NIA 315.A63 incluye ejemplos de riesgos específicos relacionados con TI. El diagrama que se muestra abajo incluye ejemplos de riesgos estándar (con base en la NIA 315) que generalmente consideramos cuando analizamos los cuatro dominios de TI. Consulte el folleto "Probar los CGTI – Evaluación de riesgos de TI" en la pestaña de recursos para ver los factores clave a considerar para evaluar los riesgos de TI más relevantes.



 [Click en los 4 dominios de TI para encontrar los riesgos cubiertos](#)

Más Información

Desarrollo de programas

- Aplicaciones recién implementadas que no procesan los datos correctamente debido a problemas de codificación o configuración.
- Problemas para migrar registros de transacciones o archivos maestros.

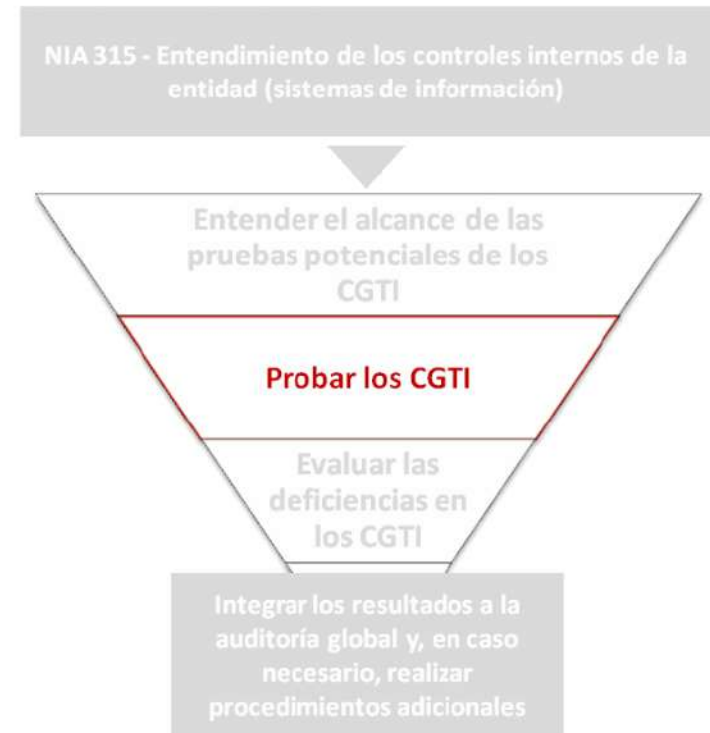
Entendiendo y respondiendo a los riesgos de TI

¿Dónde estoy?

En este módulo aprendió acerca de los factores que debe considerar cuando esté desarrollando su estrategia de pruebas para los CGTI, incluyendo:

- la complejidad de los sistemas,
- las áreas de riesgos potenciales,
- las características de un sistema complejo y no complejo y
- los 12 ejemplos de riesgos específicos de TI basados en la NIA 315.

En el próximo módulo aprenderá cómo evaluar las deficiencias en los CGTI identificadas como resultado de sus pruebas.



Entendiendo y respondiendo a los riesgos de TI



Módulo 5

En este módulo conocerá las acciones que debe tomar si encuentra deficiencias en los CGTI.

Entendiendo y respondiendo a los riesgos de TI

Evaluar el impacto de las deficiencias

? Si el equipo ha identificado una o más deficiencias en los CGTI, deberá determinar si existen controles de mitigación (en TI o el negocio) o si puede realizar procedimientos alternos para precisar si las deficiencias han sido aprovechadas indebidamente. Veamos entonces cómo la gerencia obtiene seguridad de que las deficiencias en los CGTI no han sido aprovechadas indebidamente y las acciones que debemos tomar.



Continuar



Continuar



Continuar

➔ Haga click en "Continuar" y "Regresar" para ver la conversación.

Entendiendo y respondiendo a los riesgos de TI

Evaluar el impacto de las deficiencias

? Si el equipo ha identificado una o más deficiencias en los CGTI, deberá determinar si existen controles de mitigación (en TI o el negocio) o si puede realizar procedimientos alternos para precisar si las deficiencias han sido aprovechadas indebidamente. Veamos entonces cómo la gerencia obtiene seguridad de que las deficiencias en los CGTI no han sido aprovechadas indebidamente y las acciones que debemos tomar.

➔ Haga click en "Continuar" y "Regresar" para ver la conversación.



Continuar

La Deficiencia

1 de 5

Quería hablar con usted sobre nuestros hallazgos con respecto a sus controles de TI. Notamos que la configuración de las contraseñas para entrar en el Sistema del Mayor para registrar pólizas de diario necesita ser cambiada con más frecuencia.



Continuar



Continuar

Entendiendo y respondiendo a los riesgos de TI

Evaluar el impacto de las deficiencias

? Si el equipo ha identificado una o más deficiencias en los CGTI, deberá determinar si existen controles de mitigación (en TI o el negocio) o si puede realizar procedimientos alternos para precisar si las deficiencias han sido aprovechadas indebidamente. Veamos entonces cómo la gerencia obtiene seguridad de que las deficiencias en los CGTI no han sido aprovechadas indebidamente y las acciones que debemos tomar.

➔ Haga click en "Continuar" y "Regresar" para ver la conversación.



Continuar



Continuar



Continuar

La deficiencia

1 de 5

Quería hablar con usted sobre nuestros hallazgos con respecto a los derechos de acceso. No se bloquearon los derechos de acceso de algunos egresados cuando se fueron de la compañía.

Entendiendo y respondiendo a los riesgos de TI

Evaluar el impacto de las deficiencias

? Si el equipo ha identificado una o más deficiencias en los CGTI, deberá determinar si existen controles de mitigación (en TI o el negocio) o si puede realizar procedimientos alternos para precisar si las deficiencias han sido aprovechadas indebidamente. Veamos entonces cómo la gerencia obtiene seguridad de que las deficiencias en los CGTI no han sido aprovechadas indebidamente y las acciones que debemos tomar.

➔ Haga click en "Continuar" y "Regresar" para ver la conversación.



Continuar



Continuar



Continuar

La deficiencia

1 de 5

Quería hablar con usted sobre otra inquietud relacionada con el acceso. El Contralor Financiero tiene pleno acceso a todas las funcionalidades del sistema.

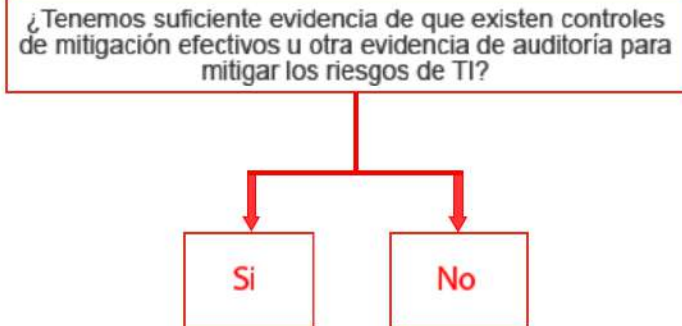
Entendiendo y respondiendo a los riesgos de TI

Determinar si el riesgo ha sido mitigado

Después de determinar el impacto de cada deficiencia en los CGTI, debe determinar si el riesgo creado por la deficiencia ha sido mitigado

Mas Información

 Click en "Si" o "No" para obtener mayor información.



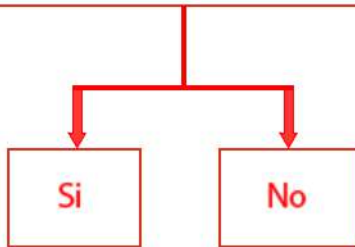
Entendiendo y respondiendo a los riesgos de TI

Determinar si el riesgo ha sido mitigado

Después de determinar el impacto de cada deficiencia en los CGTI, debe determinar si el riesgo creado por la deficiencia ha sido mitigado

 Click en "Si" o "No" para obtener mayor información.

¿Tenemos suficiente evidencia de que existen controles de mitigación efectivos u otra evidencia de auditoría para mitigar los riesgos de TI?



Mas Información


Sí

- Documente su razonamiento con base en los resultados de las pruebas realizadas.
- No se requiere trabajo adicional para TI.

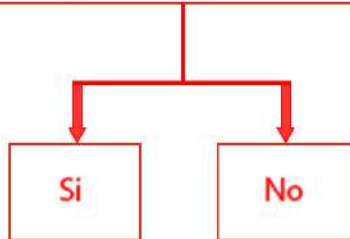
Entendiendo y respondiendo a los riesgos de TI

Determinar si el riesgo ha sido mitigado

Después de determinar el impacto de cada deficiencia en los CGTI, debe determinar si el riesgo creado por la deficiencia ha sido mitigado

 Click en "Si" o "No" para obtener mayor información.

¿Tenemos suficiente evidencia de que existen controles de mitigación efectivos u otra evidencia de auditoría para mitigar los riesgos de TI?



Mas Información

No

- Reevalúe la naturaleza, oportunidad y alcance de las pruebas sustantivas realizadas a los saldos de cuentas o transacciones afectadas .
- Considere procedimientos adicionales

Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Evaluar las deficiencias en los CGTI

La gerencia de la compañía XYZ se entera de que el personal de Tecnología puede crear cuentas de usuario nuevas (inválidas) y usarlas indebidamente.

 ¿Cuál es la respuesta correcta?

- a. Para evitar que el personal de Tecnología cree una cuenta de usuario no autorizada, la gerencia decide implementar un nuevo sistema que es más complejo. Por ende, el riesgo ha sido mitigado.
- b. La gerencia genera un reporte de todas las cuentas de usuario para verificar si existen cuentas de usuario no autorizadas y, de haberlas, si han sido usadas indebidamente. Por ende, no es necesario que realicemos pruebas adicionales para respaldar la conclusión de que el riesgo ha sido mitigado.
- c. La gerencia genera un reporte de todas las cuentas de usuario para verificar si existen cuentas de usuario no autorizadas y, de haberlas, si han sido usadas indebidamente. El equipo de auditoría realiza una conciliación para probar que no se hicieron cambios significativos en los registros.

Entendiendo y respondiendo a los riesgos de TI

Prueba de conocimientos - Evaluar las deficiencias en los CGTI

La gerencia de la compañía XYZ se entera de que el personal de Tecnología puede crear cuentas de usuario nuevas (inválidas) y usarlas indebidamente.

 ¿Cuál es la respuesta correcta?

- a. Para evitar que el personal de Tecnología cree una cuenta de usuario no autorizada, la gerencia decide implementar un nuevo sistema que es más complejo. Por ende, el riesgo ha sido mitigado.
- b. La gerencia genera un reporte de todas las cuentas de usuario para verificar si existen cuentas de usuario no autorizadas y, de haberlas, si han sido usadas indebidamente. Por ende, no es necesario que realicemos pruebas adicionales para respaldar la conclusión de que el riesgo ha sido mitigado.
- c. La gerencia genera un reporte de todas las cuentas de usuario para verificar si existen cuentas de usuario no autorizadas y, de haberlas, si han sido usadas indebidamente. El equipo de auditoría realiza una conciliación para probar que no se hicieron cambios significativos en los registros.

Entendiendo y respondiendo a los riesgos de TI

¿Donde estoy?

En este módulo aprendió qué hacer si encuentra deficiencias en los CGTI de los sistemas de información.

Específicamente, para cada deficiencia deberá evaluar si la gerencia puede demostrar que la deficiencia no ha sido aprovechada indebidamente. La gerencia podría lograr esto haciendo investigaciones o apoyándose en controles de mitigación.

Una vez que la gerencia demuestre que la deficiencia no ha sido aprovechada indebidamente, es necesario que determine si existe suficiente evidencia de auditoría compensatoria para mitigar el riesgo de TI y su impacto en el enfoque de auditoría, incluyendo el impacto en las pruebas de controles y pruebas sustantivas de ser necesario.

En el próximo módulo aprenderá a integrar los resultados de sus pruebas a la auditoría global.



Entendiendo y respondiendo a los riesgos de TI



Módulo 6

Ahora veamos cómo integrar los resultados de sus pruebas a su plan de auditoría.

Entendiendo y respondiendo a los riesgos de TI

Integrar los resultados

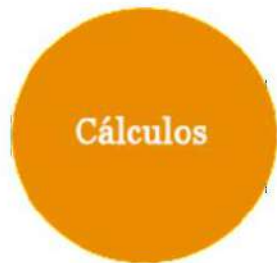
Después de probar los CGTI es necesario que considere el impacto de sus resultados en el compromiso global. Recuerde que los CGTI proporcionan evidencia indirecta de que los controles de aplicación están operando como es debido.

Hay tres conclusiones posibles con los CGTI:

1. Probarlos y concluir que puede depender de ellos. Esto implica que puede reducir el número de pruebas realizadas a los controles de aplicación.
2. Probarlos y concluir que no son efectivos y, por ende, que no puede depender de ellos.
3. Concluir que sería ineficiente probar los CGTI porque no dependerá de ellos.

Si llega a la conclusión 2 o 3 (es decir, no puede o no desea depender de los CGTI), implicaría que debe considerar procedimientos adicionales para reducir el riesgo de auditoría a niveles aceptables. El siguiente gráfico muestra algunos ejemplos de procedimientos adicionales que puede realizar para obtener evidencia de los distintos controles de aplicación.

 *Click en cada círculo para leer los procedimientos adicionales que serán necesarios*



Entendiendo y respondiendo a los riesgos de TI

Integrar los resultados

Después de probar los CGTI es necesario que considere el impacto de sus resultados en el compromiso global. Recuerde que los CGTI proporcionan evidencia indirecta de que los controles de aplicación están operando como es debido.

Hay tres conclusiones posibles con los CGTI:

1. Probarlos y concluir que puede depender de ellos. Esto implica que puede reducir el número de pruebas realizadas a los controles de aplicación.
2. Probarlos y concluir que no son efectivos y, por ende, que no puede depender de ellos.
3. Concluir que sería ineficiente probar los CGTI porque no dependerá de ellos.

Si llega a la conclusión 2 o 3 (es decir, no puede o no desea depender de los CGTI), implicaría que debe considerar procedimientos adicionales para reducir el riesgo de auditoría a niveles aceptables. El siguiente gráfico muestra algunos ejemplos de procedimientos adicionales que puede realizar para obtener evidencia de los distintos controles de aplicación.

 Click en cada circulo para leer los procedimientos adicionales que serán necesarios



Entendiendo y respondiendo a los riesgos de TI

Integrar los resultados

Después de probar los CGTI es necesario que considere el impacto de sus resultados en el compromiso global. Recuerde que los CGTI proporcionan evidencia indirecta de que los controles de aplicación están operando como es debido.

Hay tres conclusiones posibles con los CGTI:

1. Probarlos y concluir que puede depender de ellos. Esto implica que puede reducir el número de pruebas realizadas a los controles de aplicación.
2. Probarlos y concluir que no son efectivos y, por ende, que no puede depender de ellos.
3. Concluir que sería ineficiente probar los CGTI porque no dependerá de ellos.

Si llega a la conclusión 2 o 3 (es decir, no puede o no desea depender de los CGTI), implicaría que debe considerar procedimientos adicionales para reducir el riesgo de auditoría a niveles aceptables. El siguiente gráfico muestra algunos ejemplos de procedimientos adicionales que puede realizar para obtener evidencia de los distintos controles de aplicación.

 Click en cada círculo para leer los procedimientos adicionales que serán necesarios



Entendiendo y respondiendo a los riesgos de TI

Integrar los resultados

Después de probar los CGTI es necesario que considere el impacto de sus resultados en el compromiso global. Recuerde que los CGTI proporcionan evidencia indirecta de que los controles de aplicación están operando como es debido.

Hay tres conclusiones posibles con los CGTI:

1. Probarlos y concluir que puede depender de ellos. Esto implica que puede reducir el número de pruebas realizadas a los controles de aplicación.
2. Probarlos y concluir que no son efectivos y, por ende, que no puede depender de ellos.
3. Concluir que sería ineficiente probar los CGTI porque no dependerá de ellos.

Si llega a la conclusión 2 o 3 (es decir, no puede o no desea depender de los CGTI), implicaría que debe considerar procedimientos adicionales para reducir el riesgo de auditoría a niveles aceptables. El siguiente gráfico muestra algunos ejemplos de procedimientos adicionales que puede realizar para obtener evidencia de los distintos controles de aplicación.

 Click en cada círculo para leer los procedimientos adicionales que serán necesarios



Entendiendo y respondiendo a los riesgos de TI

Integrar los resultados

Después de probar los CGTI es necesario que considere el impacto de sus resultados en el compromiso global. Recuerde que los CGTI proporcionan evidencia indirecta de que los controles de aplicación están operando como es debido.

Hay tres conclusiones posibles con los CGTI:

1. Probarlos y concluir que puede depender de ellos. Esto implica que puede reducir el número de pruebas realizadas a los controles de aplicación.
2. Probarlos y concluir que no son efectivos y, por ende, que no puede depender de ellos.
3. Concluir que sería ineficiente probar los CGTI porque no dependerá de ellos.

Si llega a la conclusión 2 o 3 (es decir, no puede o no desea depender de los CGTI), implicaría que debe considerar procedimientos adicionales para reducir el riesgo de auditoría a niveles aceptables. El siguiente gráfico muestra algunos ejemplos de procedimientos adicionales que puede realizar para obtener evidencia de los distintos controles de aplicación.

 *Click en cada círculo para leer los procedimientos adicionales que serán necesarios*



Entendiendo y respondiendo a los riesgos de TI

Integrar los resultados

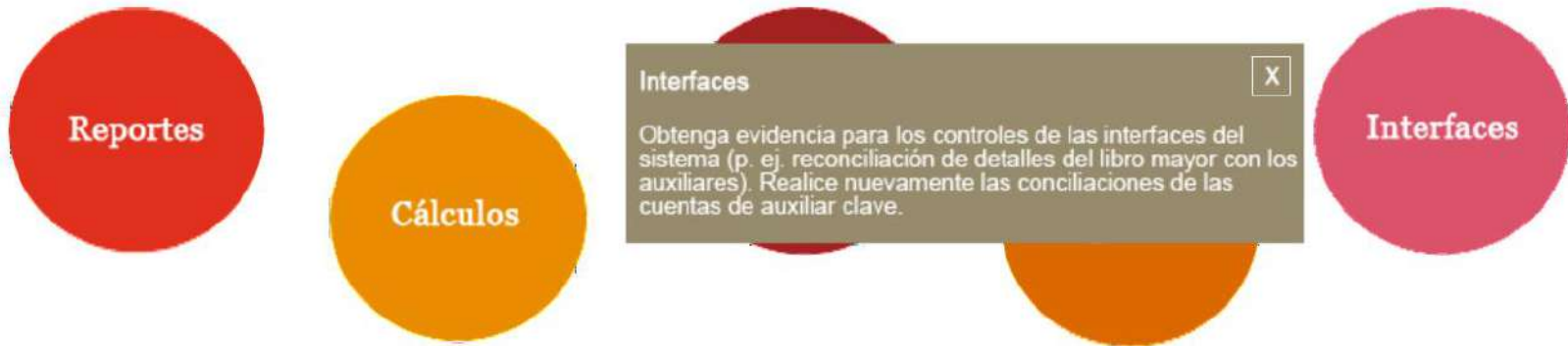
Después de probar los CGTI es necesario que considere el impacto de sus resultados en el compromiso global. Recuerde que los CGTI proporcionan evidencia indirecta de que los controles de aplicación están operando como es debido.

Hay tres conclusiones posibles con los CGTI:

1. Probarlos y concluir que puede depender de ellos. Esto implica que puede reducir el número de pruebas realizadas a los controles de aplicación.
2. Probarlos y concluir que no son efectivos y, por ende, que no puede depender de ellos.
3. Concluir que sería ineficiente probar los CGTI porque no dependerá de ellos.

Si llega a la conclusión 2 o 3 (es decir, no puede o no desea depender de los CGTI), implicaría que debe considerar procedimientos adicionales para reducir el riesgo de auditoría a niveles aceptables. El siguiente gráfico muestra algunos ejemplos de procedimientos adicionales que puede realizar para obtener evidencia de los distintos controles de aplicación.

 *Click en cada círculo para leer los procedimientos adicionales que serán necesarios*



Entendiendo y respondiendo a los riesgos de TI

¿Donde estoy?

¡Ya se encuentra en la fase final del proceso de CGTI!

En este módulo aprendió acerca del impacto que sus pruebas sobre los CGTI podrían tener en la naturaleza y alcance de pruebas adicionales. En particular:

- Si los CGTI son efectivos para mitigar los riesgos de TI, es posible reducir las pruebas realizadas a los controles de aplicación y productos del sistema (p. ej. reportes) y
- Si los CGTI no son efectivos, podría ser necesario realizar procedimientos adicionales para recopilar evidencia de auditoría, especialmente para algunos controles de aplicación.

En el próximo y último módulo, repasará todo lo que ha aprendido en el programa.



Entendiendo y respondiendo a los riesgos de TI



Módulo 7

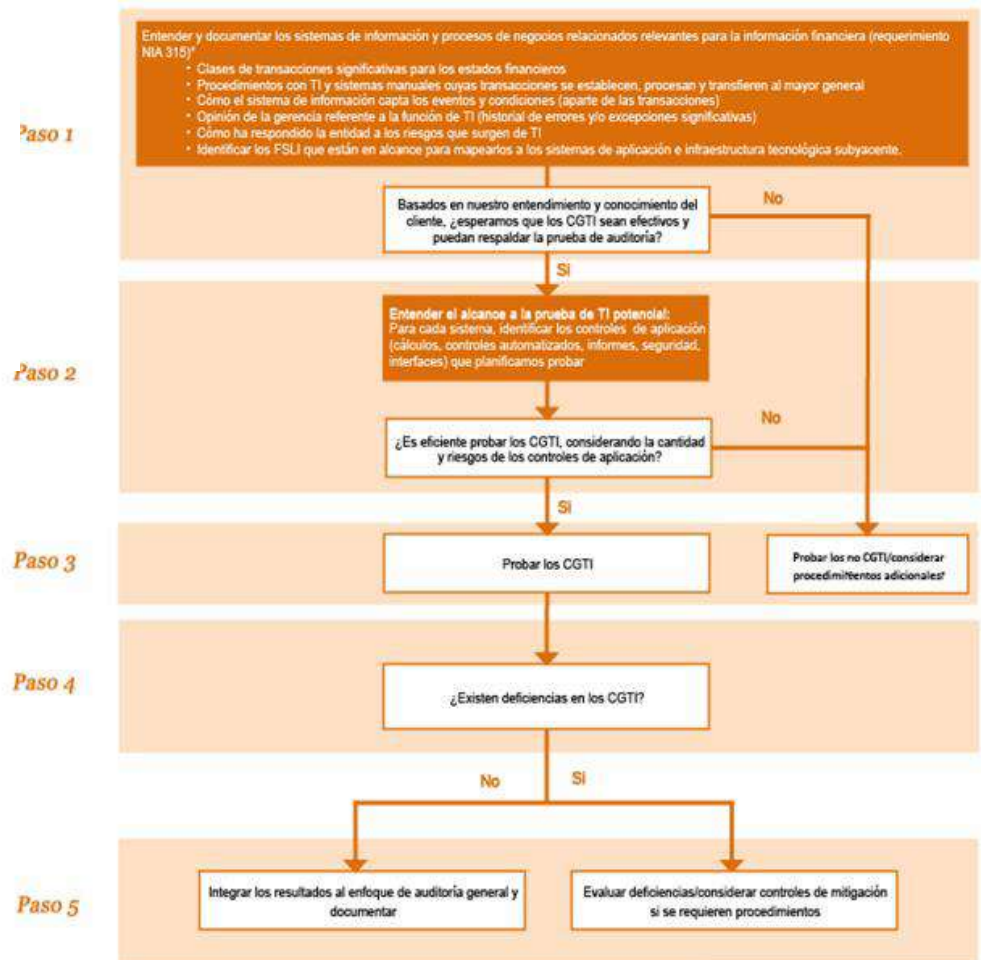
Este módulo resume el proceso de principio a fin para los CGTI.

Entendiendo y respondiendo a los riesgos de TI

Resumen

En este programa vimos una síntesis de los CGTI y repasamos la evidencia que pueden proporcionar, así como algunos de los factores que debemos considerar a la hora de diseñar un enfoque de pruebas de los CGTI para la auditoría.

El diagrama a la derecha es un árbol de decisiones que lo ayudará a tomar acciones y decisiones a través de todo el proceso de CGTI.



* Entender y documentar los sistemas de información y procesos de negocios relacionados relevantes para la información financiera (requerimiento de la NIA 315)

Entendiendo y respondiendo a los riesgos de TI

Paso 1

Entender y documentar los sistemas de información y procesos de negocios relacionados relevantes para la información financiera (requerimiento NIA 315)*

- Clases de transacciones significativas para los estados financieros
- Procedimientos con TI y sistemas manuales cuyas transacciones se establecen, procesan y transfieren al mayor general
- Cómo el sistema de información capta los eventos y condiciones (aparte de las transacciones)
- Opinión de la gerencia referente a la función de TI (historial de errores y/o excepciones significativas)
- Cómo ha respondido la entidad a los riesgos que surgen de TI

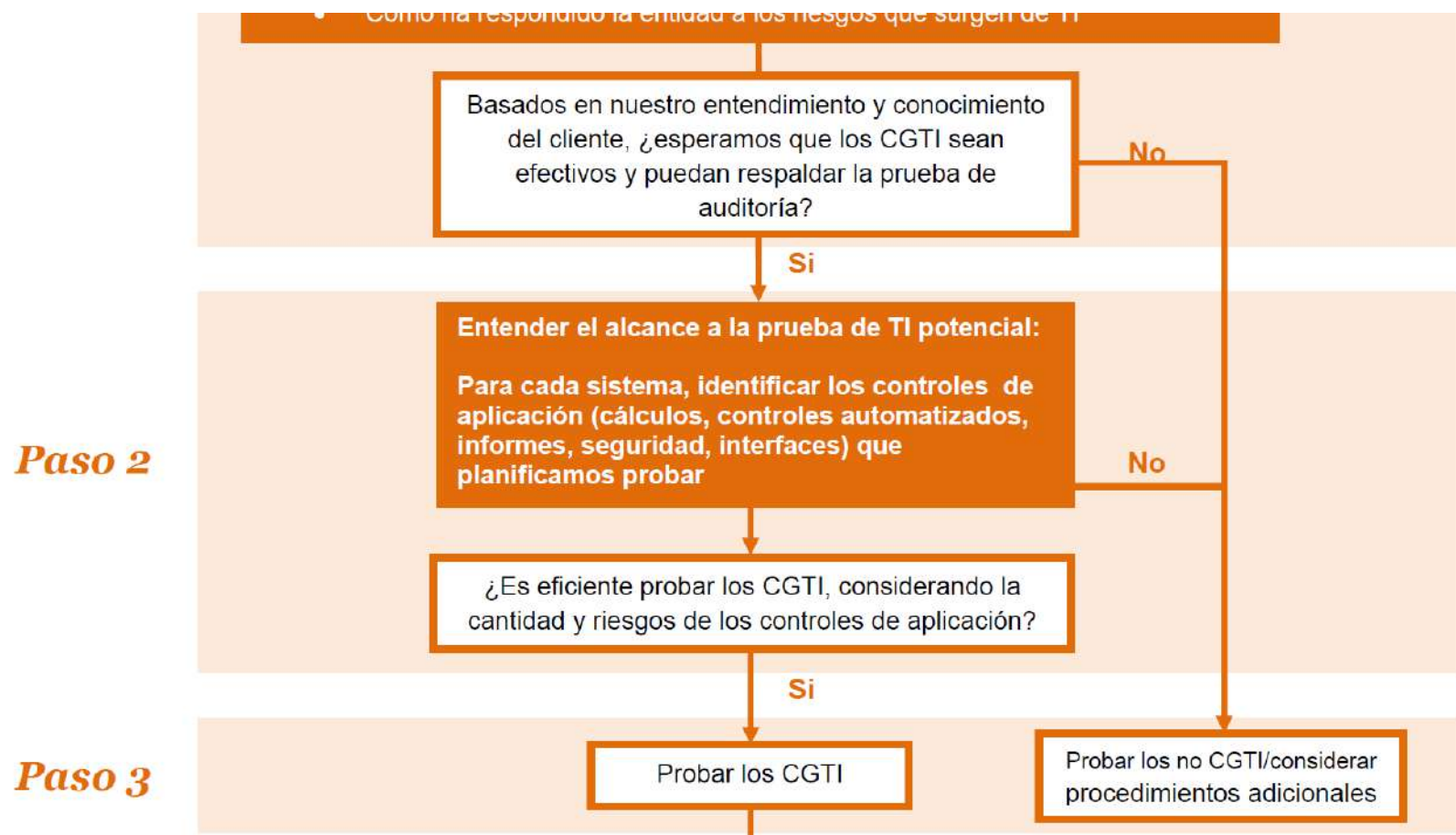
Basados en nuestro entendimiento y conocimiento del cliente, ¿esperamos que los CGTI sean efectivos y puedan respaldar la prueba de auditoría?

Si

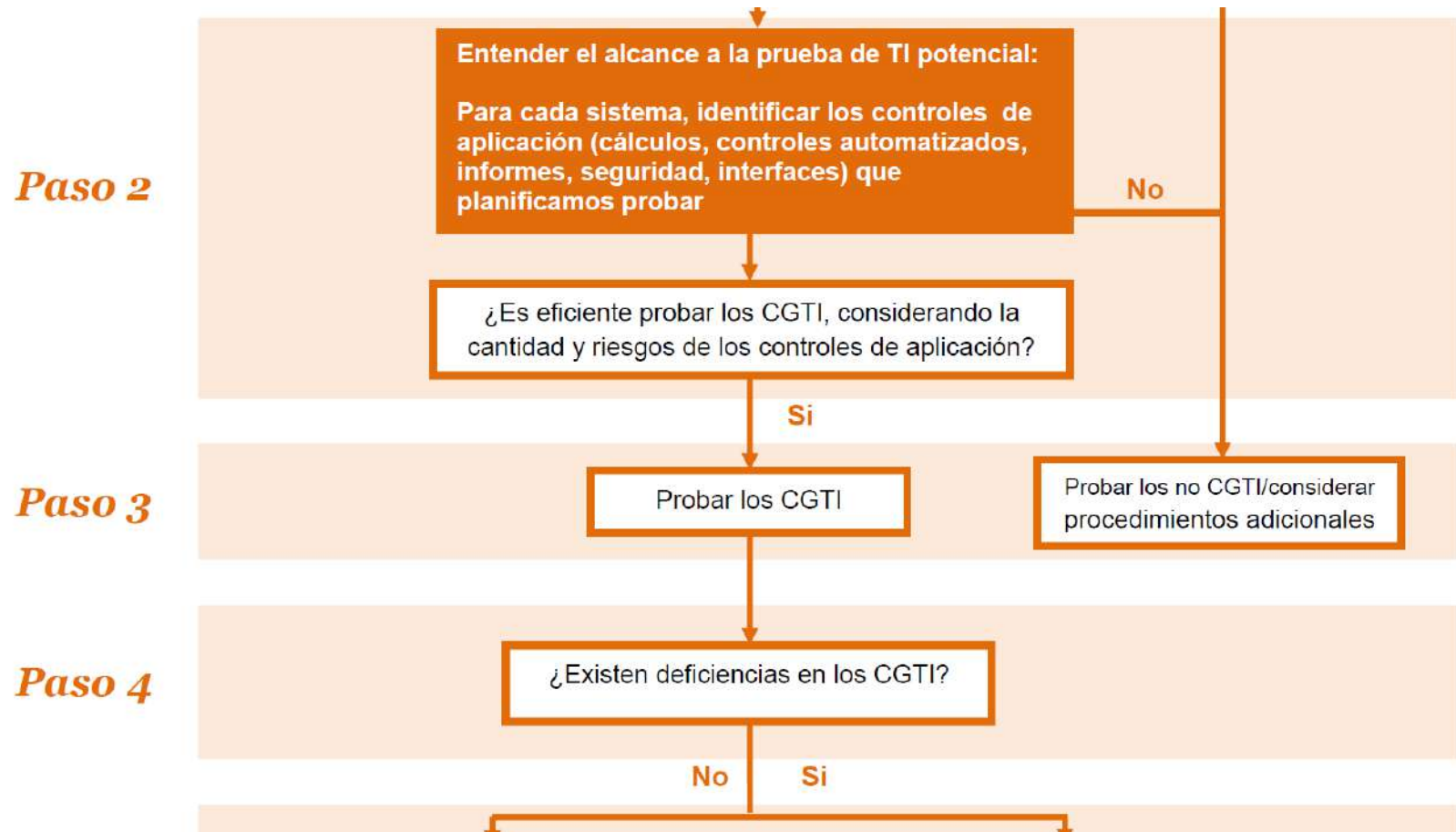
No

Entender el alcance a la prueba de TI potencial:

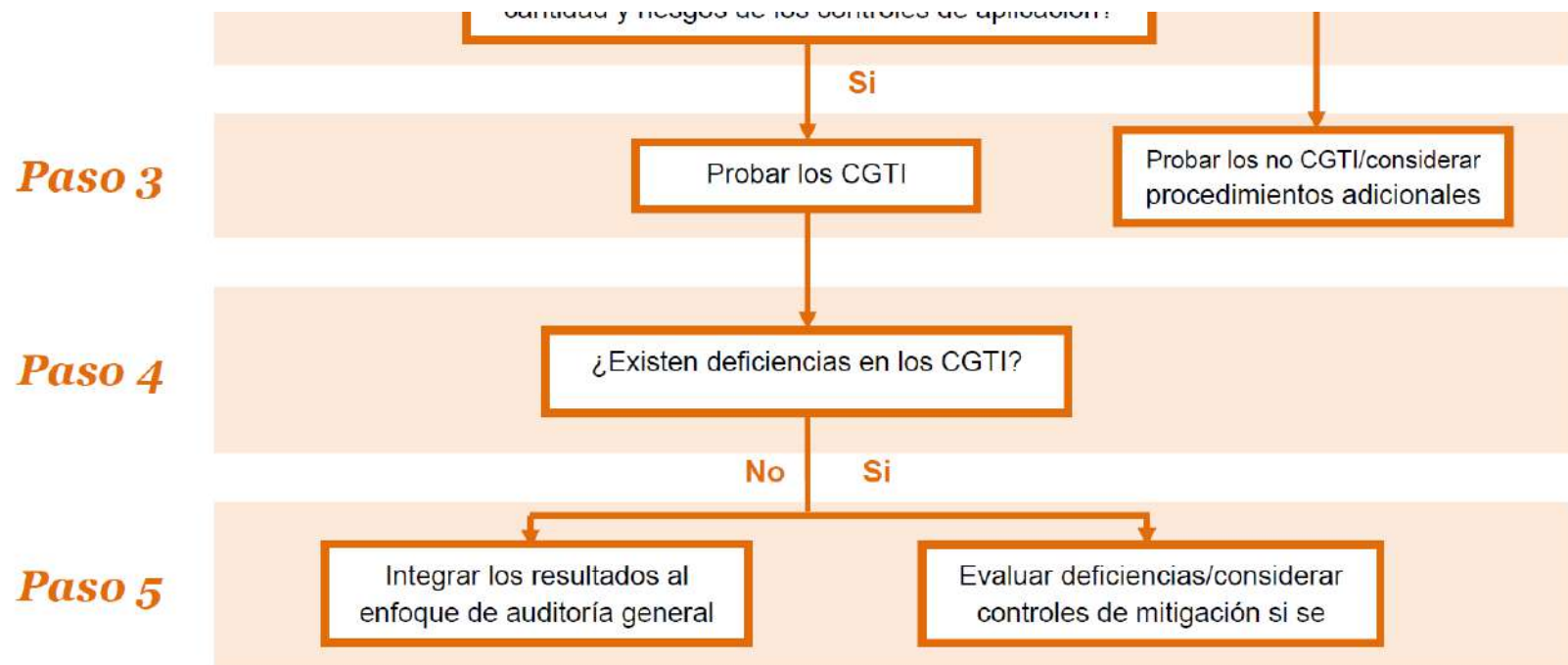
Entendiendo y respondiendo a los riesgos de TI



Entendiendo y respondiendo a los riesgos de TI



Entendiendo y respondiendo a los riesgos de TI



* Entender y documentar los sistemas de información y procesos de negocios relacionados relevantes para la información financiera (requerimiento de la NIA 315)

Entendiendo y respondiendo a los riesgos de TI

Apéndice II

Prueba de CGTI – sistemas no complejos

El plan de pruebas a continuación puede utilizarse cuando hayamos concluido que los sistemas de TI no son complejos y podemos enfocar nuestros procedimientos en pocos riesgos de TI. Sin embargo, podrían ser necesarios procedimientos adicionales dependiendo de los riesgos y circunstancias del cliente.

Riesgos	Controles	Ejemplos de procedimientos de prueba
Acceso a los programas y datos		
Usuarios de aplicaciones de negocios y TI que evitan la autorización impuesta por el sistema o los controles de separación de tareas	Parámetros/configuraciones de contraseñas son adecuados y acordes con las normas de seguridad	1 Es necesario que las contraseñas tengan por lo menos 6 caracteres y se cambien cada 90 días. Se debe confirmar por medio de indagación y revisión de las configuraciones que estas configuraciones existen. Observe el ingreso del cliente al sistema TI para confirmar que se requiere una contraseña. Considere una excepción si no se requiere una contraseña, no se configura una contraseña de 6 caracteres y ésta no expira a los 90 días o menos.
<i>Nota: si el cliente mantiene bases de datos, los procedimientos de prueba 4 y 5 son requeridos para la aplicación y la base(s) de datos.</i>	Se revisa la adecuación y la autorización por parte de la gerencia de las Solicitudes de acceso a la aplicación	2 a. Solicite al departamento de Nómina o Recursos humanos un informe del sistema con los empleados nuevos (es decir, empleados recién contratados) por el período de auditoría y del departamento de TI un informe del sistema de las cuentas de usuarios y los roles en el sistema TI. Compare los informes (es decir, con respecto a los usuarios que aparecen en los dos informes) a fin de determinar el número de cuentas de usuario recientemente creadas para el período que está en auditoría. Esta es la población del control.

Entendiendo y respondiendo a los riesgos de TI

Tareas

Nota: si el cliente mantiene bases de datos, los procedimientos de prueba 4 y 5 son requeridos para la aplicación y la base(s) de datos.

Se revisa la adecuación y la autorización por parte de la gerencia de las Solicitudes de acceso a la aplicación

2

Guías e informes.

- a. Solicite al departamento de Nómina o Recursos humanos un informe del sistema con los empleados nuevos (es decir, empleados recién contratados) por el período de auditoría y del departamento de TI un informe del sistema de las cuentas de usuarios y los roles en el sistema TI. Compare los informes (es decir, con respecto a los usuarios que aparecen en los dos informes) a fin de determinar el número de cuentas de usuario recientemente creadas para el período que está en auditoría. Esta es la población del control.
- b. Siguiendo los lineamientos referentes a los tamaños de muestra para la prueba de controles (PwC Audit 6053), obtenga y revise la solicitud de acceso de una muestra de las cuentas de usuarios nuevos y observe si los formularios fueron aprobados oportunamente por la persona adecuada (generalmente es el supervisor). Confirme si se proporcionó el acceso de usuario aprobado comparando la solicitud de acceso con la lista que contiene el nombre de la persona con acceso y rol en el informe del sistema de cuentas de usuarios y roles. Considere una excepción si no está documentada la aprobación o si el rol asignado no es el mismo que el rol aprobado.

Se eliminan oportunamente los derechos de acceso a las personas que ya no pertenecen a la empresa

3

Solicite al departamento de Nómina o Recursos humanos un informe del sistema de las personas que ya no son empleados por el período de la auditoría y del departamento de TI un informe del sistema de las cuentas de usuario y sus roles en el sistema(s) relevante. Compare los informes (es decir, para los usuarios que aparecen en los dos informes) a fin de determinar si las personas que ya no son empleados aún tienen cuentas de usuarios activas. Considere una excepción si existen ex empleados que tienen cuentas de usuarios activas.

Se revisa periódicamente la adecuación de los derechos de acceso del usuario, incluyendo super- usuarios, incluyendo la separación de tareas.

4

Para una muestra de meses o trimestres (dependiendo de la frecuencia del control), confirme si la gerencia realizó una revisión del acceso de usuarios y las acciones de seguimiento producto de la revisión. Considere una excepción si no fue realizada la revisión o si no hubo acciones de seguimiento.

Refiérase al apéndice IV para ver la definición de super-usuario

5

Revise el informe del sistema de las cuentas de usuario y sus roles para determinar cuáles empleados tiene acceso de super-usuario (Ej., roles con nombre de "ADMIN" o "SEGURIDAD" generalmente son cuentas de super-usuarios). Para cada usuario con una cuenta de super-usuario, confirme si se ha otorgado el acceso adecuado de acuerdo con los roles y responsabilidades. Considere una excepción para los empleados con acceso de super-usuarios inadecuados (Ej., un Director financiero o Director ejecutivo con una cuenta de super-usuario).

Entendiendo y respondiendo a los riesgos de TI

empleados con acceso de super-usuarios inadecuados (Ej., un Director financiero o Director ejecutivo con una cuenta de super-usuario).

Cambios del programa

Cambios erróneos o no autorizados a los programas

Se revisan y aprueban los cambios antes de hacerlos en el ambiente real

6

Preguntar al cliente cuáles han sido los cambios realizados al sistema TI durante el año (incluyendo los cambios a las configuraciones). Si no se realizaron cambios, obtenga la evidencia generada por el sistema referente a que no se realizaron cambios (Ej., imagen de pantalla con la última fecha de cambio de los programas, imagen de pantalla de las configuraciones). Verificar que el acceso para realizar cambios sea el adecuado y obtenga evidencia de respaldo.

Los cambios del programa se prueban antes de realizarlos en ambiente real

7

Solicite al cliente un listado de cambios (incluyendo cambios a la configuración) para el periodo de auditoría y evalúe la totalidad del listado. Para una muestra de cambios (refiérase a PwC Audit 6053 para ver lineamientos sobre el tamaño de muestra), obtenga y revise la documentación de cambio, incluyendo si el cambio fue aprobado y probado adecuadamente antes de ser realizado. Incluya una excepción si el cambio no fue aprobado o probado antes de ser realizado. Solicite e inspeccione un listado de las cuentas del sistema con autoridad para cambiar códigos de aplicación y configuración, confirmando que se empleen las cuentas de usuario específico y que éstas estén firmadas por el personal adecuado.

Operaciones por computadora

Falla de los sistemas que ocasiona la pérdida de los registros de transacción o incapacidad para acceder a éstos cuando es requerido

Se prueba periódicamente la viabilidad de los medios de respaldo.

8

Pregunte al cliente si se realizan respaldos periódicos y observe la evidencia generada por el sistema (Ej., una imagen de pantalla que muestra las configuraciones de respaldo) referente a que se realizaron los respaldos. Considere una excepción si no se realiza un respaldo periódico (es decir, diario o semanal). Pruebe cómo se realizaron los cambios al cronograma y qué el acceso para realizar cambios esté restringido al personal adecuado.

Nota sobre los sistemas operativos y bases de datos: En algunos ambientes no complejos, un tercero es el que mantiene los sistemas operativos y bases de datos y quién ofrece un informe de auditoría de servicio referente a los CGTI relacionados (Ej., ISAE 3402). Cuando los sistemas operativos y bases de datos se mantienen localmente, también se requerirán los procedimientos mencionados anteriormente para las bases de datos. El sistema operativo en un sistema sencillo generalmente presenta un riesgo operativo y por lo tanto, para los fines de este ejemplo, no ha sido considerado en el alcance, aunque esto podría depender de las circunstancias del compromiso.

Entendiendo y respondiendo a los riesgos de TI

Apéndice II

Ejemplos de informes generados por el sistema y técnicas de prueba

El fin de este apéndice es ofrecer algunos ejemplos y técnicas de prueba para que los equipos los consideren cuando evalúen la totalidad y exactitud de los informes. En el caso de sistemas complejos, involucre a los especialistas SPA. Éstos podrán aplicar técnicas adicionales (Ej., inspeccionar el código del programa, utilizar las CAAT para conciliar un informe modificado con el informe estándar o la información subyacente, utilizando paquetes de prueba y otras técnicas)

Entendiendo y respondiendo a los riesgos de TI

Informe	Año 1 (cliente nuevo, establecer referencia o prueba de no CGTI)*	Año 2 + (Referencia Año 1 efectivo y prueba de CGTI)**
Informe de análisis preparado por el cliente (Ej., informe de antigüedad de cuentas por cobrar)	<p>Es necesario probar la totalidad y exactitud de los informes. Esto podría incluir:</p> <ul style="list-style-type: none"> • Aplicar prueba de aceptación-rechazo en la fecha y monto de las transacciones individuales para los documentos de respaldo (facturas de ventas, y si es adecuado, documentos de envío) para verificar la exactitud del informe de las cuentas por cobrar y la antigüedad • Comparar el saldo total en el informe con el monto en el mayor general para verificar que no existen partidas faltantes • Uso de CAAT para probar la precisión matemática y la totalidad del informe (es decir, redeseñe del informe) 	<p>Cuando se realizó una prueba en un período anterior, no es necesario realizar la prueba del diseño del informe cada año siempre que el equipo de compromiso obtenga evidencia de que no se han realizado cambios al informe. Si se ha modificado el informe desde la última vez que fue probado es necesario que obtengamos evidencia de auditoría referente a la integridad de los cambios.</p> <p>La prueba del segundo año y posteriores incluye la observación de parámetros utilizados para realizar el informe.</p>
Informes de excepción (Ej., un listado de los pagos que exceden el límite máximo especificado en el grupo de tolerancia)	<p>La prueba para verificar la totalidad de estos informes variará dependiendo de su naturaleza. Cuando se decida el enfoque para la prueba considere:</p> <ul style="list-style-type: none"> • Inspección de los parámetros usados para producir el informe 	<p>Cuando se realizó la prueba en un período anterior, no es necesario realizar esta prueba cada año debido siempre y cuando el equipo de compromiso esté satisfecho con respecto a que no se realizaron cambios significativos en los sistemas o ambiente de control del cliente.</p>

Entendiendo y respondiendo a los riesgos de TI

Informes de excepción (Ej., un listado de los pagos que exceden el límite máximo especificado en el grupo de tolerancia)
Informes de transacción rechazados (Ej., débitos directos fallidos) listado de las transacciones que cumplen con atributos definidos previamente (Ej., construcción-adiciones en progreso para un período definido)

La prueba para verificar la totalidad de estos informes variará dependiendo de su naturaleza. Cuando se decida el enfoque para la prueba considere:

- Inspección de los parámetros usados para producir el informe
- Inspección de los controles de aplicación (Ej. Numeración secuencial de un tipo de documento particular)
- Trabajar con el cliente para producir un informe que se comparará con el balance de comprobación y que podríamos luego filtrar nosotros mismos (es decir, redesepeño)

La manera más eficiente de probar la exactitud matemática de informes grandes es obtener un informe electrónicamente y utilizar Excel, Access u otro software para el total y sub-totales y/o el gran total del informe.

Cuando se realizó la prueba en un período anterior, **no** es necesario realizar esta prueba cada año debido siempre y cuando el equipo de compromiso esté satisfecho con respecto a que no se realizaron cambios significativos en los sistemas o ambiente de control del cliente.

Si se ha modificado el informe desde la última vez que fue probado es necesario obtener evidencia de auditoría referente a la integridad de los cambios. La prueba del segundo año y posteriores **incluye** la observación de parámetros utilizados para realizar el informe.

() Si los CGTI no son confiables o no fueron probados, es necesario que probemos sustantivamente la información **tantas veces como utilicemos el informe**. Por ejemplo, si se prueba sustantivamente la antigüedad de cuentas por cobrar en una fecha interina y al final del año, es necesario probar dos veces el informe de antigüedad; **una vez en una fecha interina y otra vez al cierre del año**.*

*(**) Esto aplica únicamente a la prueba de los CGTI en la aplicación en cuestión. Por ejemplo, si el informe es generado de un sistema o aplicación que no está en alcance para los fines de los CGTI, realice los procedimientos señalados en la columna "prueba para no CGTI"*

Recuerde:

- La prueba de los CGTI no implican necesariamente que los informes generados por el sistema sean confiables
- Cualquier informe podría ser estándar, estar codificados o configurado:
 - Un informe estándar está predefinido en el sistema (la lógica del informe no puede cambiarse)
 - Los informes codificados son aquellos que están incluidos en el código fuente del sistema; la capacidad de hacer cambios en el informe probablemente esté limitada a los especialistas técnicos (es decir, personal TI) y no pueden ser realizados directamente por los usuarios de la empresa y
 - Los informes configurados son aquellos que probablemente modifiquen los usuarios del sistema (establecer parámetros/rango de fecha o agregar/eliminar campos de información)
- Se podría considerar que un informe está completo y matemáticamente preciso si obtenemos suficiente evidencia de auditoría adecuada sobre incapacidad del cliente para acceder o cambiar la lógica del informe. En estos casos no se requiere ninguna prueba adicional. Si no existe suficiente evidencia, es necesario aplicar algunas de las técnicas descritas en la tabla.
 - Si es adecuado, los equipos podrían confiar en la prueba de los informes generados por el sistema realizada por la gerencia.

Entendiendo y respondiendo a los riesgos de TI

Appendix I

Test ITGCs – IT risk assessment

The guidance below can be used to understand the key factors to consider when assessing the relevant IT risks. However, additional procedures may be necessary depending on the clients' risks and circumstances.

Domain	Risk	Considerations for the audit	Non-relevance of this risk
Access to programs and data	Normal business application users bypassing systems-enforced authorization or segregation of duties controls.	Unauthorised access to data that may result in destruction of data or improper changes to data, including the recording of unauthorized, non-existent or inaccurate transactions.	Risk may not be relevant if we are not relying on access-dependent controls for financial audit purposes. This might be if none is identified or because other audit evidence may eliminate the need: <ul style="list-style-type: none">• Reconciliations can prove that no material change has been made to records; and• Authorisation and/or segregation of duties controls to mitigate the risk of fraud are manual and do not depend on user access rights within applications.
	IT personnel or other user access administrators bypassing normal access controls and segregation of duties.	The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties. IT personnel or other user access administrators could potentially bypass normal access controls and segregation of duties by giving themselves inappropriate access rights, creating new (invalid) user accounts and then misusing them, or cracking the authentication for existing user accounts and then misusing these accounts, etc.	Risk may not be relevant if we are not relying on access-dependent controls for financial audit purposes. Other audit evidence may eliminate the need: <ul style="list-style-type: none">• Reconciliations can prove that no material change has been made to records; and• Authorisation and/or segregation of duties controls to mitigate the risk of fraud are manual and do not depend on user access rights within applications.

Entendiendo y respondiendo a los riesgos de TI

	for existing user accounts and then misusing these accounts, etc.	rights within applications.
	<p>Improper direct changes to underlying transaction records and/or master files.</p> <ul style="list-style-type: none"> • Unauthorised changes to data in master files • Unauthorised access to data (bypassing the application and its controls) that may result in destruction of data or improper changes to data, including the recording of unauthorized, non-existent or inaccurate transactions. 	<p>Risk may not be relevant if the data held on master files does not pose a risk to financial reporting. Otherwise, if master data files are routinely maintained or their impact is obvious (e.g. VAT rate), the risk assessment will typically be normal.</p>
Program changes	<p>Failure to make necessary changes to systems or programs.</p> <p>Failure to make necessary changes to systems or programs (e.g. new regulations, accounting standards and/or business processes) that could give rise to a material misstatement.</p>	<p>Risk may not be relevant if either:</p> <ol style="list-style-type: none"> a. No changes to accounting standards, regulation and/or business processes that impact financial reporting, or b. We have carried out substantive tests (e.g. scan review, tests of details) to directly check that all required changes have been made.
	<p>Changes that introduce errors into applications.</p> <p>Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both including when an application is changed, there is a risk that the change introduces errors in the processing, which could be because requirements were misunderstood and this was not picked up in testing.</p>	<p>Risk may not be relevant if we can be satisfied with appropriate evidence to demonstrate that no changes have been made to applications that are audit significant during the year.</p>
	<p>Unauthorised direct changes to application code, bypassing change control.</p> <ul style="list-style-type: none"> • Unauthorized changes to systems or programs • The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties • If applications are maintained in-house or maintained by third parties, the risk is that developers, support teams or third parties can bypass change control and make directly change/unauthorised changes to application code in production system. 	<p>Risk may not be relevant if audit significant applications are packaged systems with no in-house development/coding and third party developers cannot make changes without the client's permission or the client can demonstrate (e.g. through change logs) that no such changes have been made.</p>
	<p>Unauthorised direct changes to application configuration settings, bypassing change control.</p> <ul style="list-style-type: none"> • Unauthorized changes to systems or programs • The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties • Users or support teams may bypass change control and make unauthorised changes to application configuration settings which could be by directly changing settings in the production (live) environment. 	<p>Risk may not be relevant if the automated functions we plan to rely on are not configurable through application configuration settings (i.e. are controlled by core application code) or the client can demonstrate (e.g. through change logs) that no changes to the application settings have been made.</p>

Entendiendo y respondiendo a los riesgos de TI

	<p>Unauthorised direct changes to application configuration settings, bypassing change control.</p>	<ul style="list-style-type: none"> • Unauthorized changes to systems or programs • The possibility of IT personnel gaining access privileges beyond those necessary to perform their assigned duties thereby breaking down segregation of duties • Users or support teams may bypass change control and make unauthorised changes to application configuration settings which could be by directly changing settings in the production (live) environment. 	<p>Risk may not be relevant if the automated functions we plan to rely on are not configurable through application configuration settings (i.e. are controlled by core application code) or the client can demonstrate (e.g. through change logs) that no changes to the application settings have been made.</p>
	<p>Updates to the IT environment (IT infrastructure, operating system and system utilities) prevent applications from running correctly.</p>	<p>Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both.</p>	<p>Risk may not be relevant if the only changes to the IT environment have been routine vendor-supplied patches or fixes at the operating system layer; and there is no history of susceptibility of audit- significant applications to IT environment upgrades.</p>
Program development	<p>Newly implemented applications inaccurately process data, due to coding or configuration issues.</p>	<p>Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both which could be because requirements were misunderstood and this was not picked up in testing, or because a conscious decision was taken to go live despite known problems.</p> <p>If this risk materialises, we may not be able to rely on automated accounting procedures, controls or reports in the new application.</p>	<p>Risk may not be relevant if no new audit-significant applications were implemented during the year.</p>
	<p>Errors in migrating transaction records and/or master files.</p>	<p>Reliance on systems or programs that are inaccurately processing data, processing inaccurate data, or both which typically arises when data is converted or migrated from one data format to a new one.</p>	<p>Risk may not be relevant if no material audit-significant data has been transferred or transformed.</p>
Computer operations	<p>Inappropriate manual intervention or failures in batch processes.</p>	<p>Inappropriate manual intervention. The main area of manual intervention is in the resolution of errors in batch processes. Undetected errors could impact the completeness or accuracy of records.</p>	<p>Risk may not be relevant if there are no batch processes that are significant to the completeness and accuracy of financial data; or there are end-to-end reconciliations that prove data has been processed completely and accurately.</p>
	<p>Systems failure causing loss of transaction records or inability to access them as required.</p>	<p>Potential loss of data or inability to access data as required which includes any data corruption or processing interruption resulting in the integrity of financial records being materially compromised as a result, the organisation could be missing information needed to produce complete and accurate financial statements.</p>	<p>Risk may not be relevant if applications are stable, with low levels of downtime, no material backlog of unprocessed transactions and/or no significant data recoveries being made in the period.</p>

Add closing statement here...

Esta publicación ha sido preparada para una orientación general acerca de asuntos de interés solamente, y no constituye asesoramiento profesional. Los receptores de la misma no deben actuar en base a la información contenida en esta publicación sin obtener asesoramiento independiente. No se efectúa manifestación ni se otorga garantía alguna (expresa o implícita) con respecto a la exactitud o integridad de la información contenida en esta publicación y, en la medida en que lo permite la ley, PwC, sus miembros, empleados y agentes no aceptan ni asumen ninguna responsabilidad, ni deber de cuidado por cualquier consecuencia de su accionar, o del accionar de terceros, o de negarse a actuar, confiando en la información contenida en esta publicación, o por ninguna decisión basada en la misma.

© 2020 PricewaterhouseCoopers S.R.L. Todos los derechos reservados. "PwC" se refiere a PricewaterhouseCoopers S.R.L., firma miembro de PricewaterhouseCoopers International Limited, cada firma miembro es una entidad legal separada.