



AUDIdeas

*Publicacion Mensual con ideas para el Mejoramiento en
Gestion de Riesgos, Seguridad y Auditoría*

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 1

TEMA: USO DE RESULTADOS DE LA GESTION DE RIESGOS EN LA PLANEACION ANUAL DE AUDITORIA INTERNA

Contenido

INTRODUCCIÓN.....	2
1. CÓMO ELABORAR EL PLAN ANUAL AUDITORIA INTERNA BASADA EN VALORACIÓN DE RIESGOS?.....	3
2. INFORMACIÓN QUE PROVEEN LAS MATRICES DE RIESGO PARA EL PLAN ANUAL DE AUDITORIA INTERNA BASADA EN RIESGOS.....	5
3. EJEMPLOS DE CUESTIONARIO DE FACTORES DE RIESGO.....	6
3.1 Factores de Riesgos y Criterios de Evaluación con información Extraída de las Matrices de Riesgo.	6
3.2 Factores de Riesgos y Criterios de Evaluación con información No Extraída de las Matrices de Riesgo.	8



AUDIdeas

Publicación Mensual con ideas para el Mejoramiento en Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 2

TEMA: USO DE RESULTADOS DE LA GESTION DE RIESGOS EN LA PLANEACION ANUAL DE AUDITORIA INTERNA

USO DE RESULTADOS DE LA GESTION DE RIESGOS EN LA PLANEACION ANUAL DE LA AUDITORIA INTERNA

INTRODUCCIÓN.

Los estándares del IIA establecen que el plan anual de Auditoría Interna debe elaborarse *basado en valoración de riesgos*. Esto implica que la Auditoría Interna (o la oficina de control interno en el sector público) conozca y se apalanque en información disponible en las matrices de riesgo de la organización sobre riesgos estratégicos, operativos y de la información de los procesos del modelo de operación (estratégicos, misionales y de soporte), de los procesos de tecnología de información y de las Aplicaciones de Computador que soportan los procesos del “core del negocio”. Cuando la Empresa dispone de una infraestructura de Gestión de Riesgos Empresariales, esta información deberá estar disponible en las matrices de riesgos que resultaron de implantar sistemas de administración de riesgos tales como SARO, SARLAFT y otros subsistemas de riesgos financieros.

Pasos para Elaborar el Plan Anual de Auditoría Interna “Basado en Riesgos”



Marco Internacional para la Práctica Profesional de la Auditoría Interna del IIA.

➤ 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 auditor 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 y comunicar el impacto de cualquier limitación de recursos.

Webinar: Planeación Anual de la Auditoría “Basada en Riesgos”

8





AUDIdeas

Publicación Mensual con ideas para el Mejoramiento en Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 3

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

Cuando la organización no dispone de matrices de riesgo o de información generada por la gestión de riesgos empresariales, la Auditoría Interna deberá sustituir la falta de esta información para realizar su plan anual basado en valoración de riesgos.

1. CÓMO ELABORAR EL PLAN ANUAL AUDITORIA INTERNA BASADA EN VALORACIÓN DE RIESGOS?

Para elaborar el Plan Anual de Auditoría Basado en Valoración de Riesgos se requiere la disponibilidad de tres (3) pilares sobre los que se soporta la construcción del plan:

- a) **El Universo de Trabajos de Auditoría Interna.** Comprende el inventario de revisiones o trabajos que corresponde realizar a la Auditoría Interna, de acuerdo con el rol asignado por los estándares del IIA. Normalmente este universo está integrado por elementos de tres (3) componentes: a) los procesos del modelo de operación de la empresa (estratégicos, misionales y de soporte); b) los procesos de Tecnología de Información (TI); y c) las aplicaciones de computador que soportan las operaciones del CORE del negocio.
- b) **El Universo de Riesgos potenciales de la Empresa.** Comprende el inventario de eventos de riesgo inherente identificados en las matrices de riesgo de la empresa, para cada uno de los elementos del universo de auditoría interna. En su lugar, pueden utilizarse los nombres de las categorías o clases de riesgo consideradas por sistemas de administración de riesgo aplicables a la empresa, tales como el Sistema de Administración del Riesgo Operativo (SARO), de administración de riesgos de lavado de activos y financiación del terrorismo (SARLAFT) y por las clase de riesgos mencionados en la Guía de Administración de Riesgos del sector público colombiano.
- c) **Cuestionarios de Factores de Riesgo.** Se construyen con el propósito de estimar la exposición a riesgos de los elementos de los tres (3) componentes del universo de auditoría, de acuerdo con las respuestas obtenidas en los cuestionarios y las categorías de riesgo que son impactadas por cada pregunta de los cuestionarios. En la metodología de AUDIRISK, se proponen tres tipos de cuestionarios, uno para cada componente del universo de auditoría, es decir: uno para los procesos del

AUDITORIA INTEGRAL Y SEGURIDAD DE SISTEMAS DE INFORMACIÓN "AUDISIS"

Servicios Especializados en Prevención y Reducción de Riesgos, Seguridad y Auditoría de Sistemas

Calle 53 No. 27 - 33 Ofc. 602 –Tels. (571) 2 55 67 17 - PBX (571) 3470022 - Correo electrónico

audisis@audisis.com Sitio web: www.audisis.com - www.softwareaudisis.com

32 Años: Fundada en 1.988



AUDIideas

Publicación Mensual con ideas para el Mejoramiento en Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 4

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORÍA INTERNA

modelo de operación de la empresa; otro para los procesos de Tecnología de Información (TI); y otro para las aplicaciones de computador. La exposición a riesgos de cada elemento del universo de auditoría es un número que varía entre cero (0) y cien (100).

Cada pregunta de los cuestionarios corresponde a un factor de riesgo, con una ponderación de su importancia dentro del cuestionario y múltiples opciones de respuesta, de las cuales se pueden seleccionar una o más. Cada respuesta seleccionada tiene un peso asignado (entre 0 y 100) que multiplicada por la ponderación asignada al factor indica la exposición a riesgos del factor. La suma de las exposiciones a riesgo de cada factor de riesgo o pregunta del cuestionario, indicará la exposición total a riesgos de elemento del universo de auditoría (proceso o sistema) al que se aplica el cuestionario.

El puntaje de exposición a riesgos de cada elemento del universo de auditoría se expresa como un *porcentaje de propensión a riesgos o de seguridad requerida*. Entre más cerca esté al 100%, mayor es la propensión a riesgos o seguridad requerida; entre más cerca este a cero, menor es la exposición a riesgos o seguridad requerida.

Con los puntajes de exposición a riesgos obtenidos, los elementos de cada componente del universo de auditoría se ordenan de mayor a menor exposición a riesgos o de seguridad requerida. Los de mayor puntaje deberían tener la mayor prioridad para ser incluidos en el plan anual de auditoría.

Cuando para todos los elementos del universo de auditoría se tenga disponible un puntaje de exposición a riesgos o de seguridad requerida, los auditores asignan una prioridad a cada elemento del universo de auditoría para el plan anual de auditoría (1: la máxima, por ejemplo) y seleccionan los elementos que se incluirán en el plan anual.

Por cada elemento del universo seleccionado para el Plan Anual de Auditoría Interna, los auditores definen los trabajos que se realizarán durante el año. Por ejemplo, para un proceso seleccionado pueden programarse cuatro (4) trabajos, así:

- i. Auditoría al control interno existente en el proceso; este trabajo se realizará en las oficinas centrales de la Auditoría.
- ii. Pruebas de auditoría en múltiples sitios de operación del proceso, a los controles y la información del proceso. Para realizar pruebas de auditoría



AUDIideas

Publicación Mensual con ideas para el Mejoramiento en
Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 5

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

a un proceso, es requisito haber terminado la evaluación de control interno del proceso. El diseño y planeación de las pruebas se realizan en las oficinas centrales de la Auditoría Interna.

- iii. Seguimiento a los hallazgos de la Auditoría de Control Interno del proceso.
- iv. Seguimiento a los hallazgos de las Pruebas de Auditoría al proceso en múltiples sitios de operación.

También pueden programarse *pruebas de auditoría a Múltiples Procesos en un sitio de operación* (pruebas a los controles y la información). Por ejemplo, en una cooperativa o en un banco podrían programarse trabajos para cinco procesos (x, y, z, a y b) para realizarse en varios sitios de operación (agencias o sucursales).

2. INFORMACIÓN QUE PROVEEN LAS MATRICES DE RIESGO PARA EL PLAN ANUAL DE AUDITORIA INTERNA BASADA EN RIESGOS.

Las matrices de riesgo contienen información valiosa como ayuda para medir (estimar) la exposición a riesgo de cada proceso o sistema del universo de auditoría.

Las matrices de riesgos proveen datos de la gestión de riesgos por proceso o por subsistemas de gestión de riesgos que pueden utilizarse como insumos para construir y responder preguntas de los cuestionarios de factores de riesgo, como los datos que se mencionan a continuación:

Por cada proceso.

1. Enunciados o descripción de los eventos de riesgo inherente.
2. El valor total de los activos impactados por cada evento de riesgo.
3. Los agentes generadores del riesgo y las vulnerabilidades (causas) que crean el ambiente propicio para la ocurrencia del riesgo.
4. Las fuentes u orígenes del riesgo, es decir, de las actividades del proceso y áreas de la empresa o terceros en donde puede originarse el riesgo.



AUDIdeas

Publicación Mensual con ideas para el Mejoramiento en
Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 6

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

5. Evaluación de la Severidad de cada uno de los eventos de riesgo inherente ANTES DE CONTROLES (E: Extremo; A: Alto; M: Moderado; ó B: Bajo).
6. Por cada evento de riesgo inherente, la identificación y descripción de los controles establecidos para reducir el impacto o la probabilidad de ocurrencia del riesgo o de los tratamientos de riesgo que estén en proceso de implantación.
7. Evaluación de la Severidad de cada uno de los eventos de riesgo inherente DESPUES DE CONTROLES (E: Extremo; A: Alto; M: Moderado; ó B: Bajo), es decir, del Riesgo Residual.
8. El riesgo residual neto del proceso.
9. El valor de la Perdida simple (PS) estimada por cada ocurrencia del evento de riesgo, antes y después de controles.
10. La frecuencia anual de ocurrencia (FAO) estimada para cada evento de riesgo, antes y después de controles.
11. El valor de la pérdida anual estimada (PAE) por cada evento de riesgo inherente, antes y después de controles

Con los datos arriba mencionados, los auditores pueden diseñar preguntas y respuestas (criterios de evaluación con los cuales se mide la exposición a riesgos de cada factor de riesgo) para los cuestionarios de factores de riesgo con los cuales se estima la exposición del proceso a riesgos potenciales (o la seguridad requerida por el proceso)

3. EJEMPLOS DE CUESTIONARIO DE FACTORES DE RIESGO.

3.1 Factores de Riesgos y Criterios de Evaluación con información Extraída de las Matrices de Riesgo.

Factor de riesgo 1.

1. Cantidad de Riesgos Inherentes identificados y evaluados para el proceso.

No	Respuestas – Criterios de Evaluación	Exposición a Riesgos
a)	Entre el 20 y 30.	10
b)	Entre el 10 y 20	20
c)	Entre 5 y 10	80
d)	Menos de 5	70



AUDIideas

Publicación Mensual con ideas para el Mejoramiento en
Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 7

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

Factor de riesgo 2.

2. El porcentaje de riesgos inherentes del proceso ubicados en los niveles de severidad E: Extremo y A: Alto.

No	Respuestas – Criterios de Evaluación	Exposición a Riesgos
a)	Entre el 5% y el 20%.	10
b)	Entre el 20 y el 50%	20
c)	Entre el 50 y el 70%	50
d)	Más del 50%	80

Factor de Riesgo 3.

3. Efectividad total estimada de los controles establecidos para mitigar los riesgos inherentes del proceso.

No	Respuestas – Criterios de Evaluación	Exposición a Riesgos
a)	La Pérdida Anual Estimada (PAE) antes de controles se reduce entre el 5% y el 20%.	10
b)	La Pérdida Anual Estimada (PAE) antes de controles se reduce entre el 20 y el 50%	20
c)	La Pérdida Anual Estimada (PAE) antes de controles se reduce entre el 50 y el 70%	60
d)	La Pérdida Anual Estimada (PAE) antes de controles se reduce más del 70%	80

Factor de riesgo 4.

4. El porcentaje de controles Preventivos respecto al total de controles establecidos para los riesgos inherentes del proceso (sin repetición)

No	Respuestas – Criterios de Evaluación	Exposición a Riesgos
a)	Más del 30%	10
b)	Entre el 20 y el 30%	50
c)	Entre 0 y 20%	80



AUDIideas

Publicación Mensual con ideas para el Mejoramiento en
Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 8

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

Factor de Riesgo 5.

El porcentaje de Riesgos del proceso que tienen asignado un número plural de controles (más de un control para mitigar el riesgo)

No	Respuestas – Criterios de Evaluación	Exposición a Riesgos
a)	Más del 70%	10
b)	Entre el 50 y el 70%	20
c)	Entre el 20 y el 50%	40
d)	Entre el 0% y el 20%.	80

Factor de Riesgo 6.

El porcentaje de Riesgos del proceso que tienen controles establecidos en tres anillos de protección que hacen sinergia (al menos un control preventivo, uno detectivo y otro correctivo)

No	Respuestas – Criterios de Evaluación	Exposición a Riesgos
a)	Más del 70%	10
b)	Entre el 50 y el 70%	20
c)	Entre el 20 y el 50%	40
d)	Entre el 5% y el 20%.	80

3.2 Factores de Riesgos y Criterios de Evaluación con información No Extraída de las Matrices de Riesgo.

Normalmente los cuestionarios de valoración de exposición a riesgos contienen preguntas sobre otros factores de riesgo que no dependen de las matrices de riesgos, como los siguientes:

- Tipo de proceso;
- Convertibilidad de los activos a dinero efectivo;
- Cantidad de sitios de operación;
- Fecha última auditoría;
- Incidentes ocurridos en el último año (fraudes, de control interno, quejas y reclamos);
- Cambios recientes efectuados al proceso;
- importancia relativa o Materialidad de los activos (pasivos) manejados por el proceso;



AUDIideas

Publicación Mensual con ideas para el Mejoramiento en Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag. 9

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

- h) Dependencia de las operaciones del proceso con respecto a la Tecnología de Información.
- i) Importancia estratégica de la información que maneja.

Ejemplos de Preguntas para el Cuestionario.

Factor de Riesgo 7.

Convertibilidad a dinero efectivo, de los recursos y activos que se manejan en el proceso (Títulos Valores, Información y secreto profesional entre otros).

Criterios de evaluación	Exposición a Riesgos
De Difícil convertibilidad	10
Moderada dificultad para convertirlos en dinero efectivo	60
Fácilmente convertibles a dinero efectivo	100

Factor de Riesgo 8.

Dependencia de las operaciones del proceso con respecto a la Tecnología de Información

No	Criterios de evaluación	Exposición a Riesgos
a)	La realización de las operaciones NO DEPENDE del funcionamiento de los sistemas de TIC. Las operaciones se realizan sin ayuda de los sistemas de TIC.	10
b)	La realización de las operaciones DEPENDE PARCIALMENTE del funcionamiento de los sistemas de TIC. Sin la disponibilidad de sistemas las operaciones no pueden realizarse.	60
c)	La realización de las operaciones DEPENDE SIGNIFICATIVAMENTE del funcionamiento de los sistemas de TIC. Sin sistemas las operaciones no pueden realizarse.	100



AUDIideas

Publicación Mensual con ideas para el Mejoramiento en
Gestión de Riesgos, Seguridad y Auditoría

Bogotá D.C., Enero de 2020

Año 10 No. 1

Pag.

10

TEMA: USO DE RESULTADOS DE LA GESTIÓN DE RIESGOS EN LA PLANEACIÓN ANUAL DE AUDITORIA INTERNA

Factor de Riesgo 9.

Cantidad de puntos de operación o de servicio que originan transacciones (información) para las operaciones del proceso.

No	Criterios de evaluación	Exposición a Riesgos
a)	Menos de cinco (5)	30
b)	Entre 6 y 10	60
c)	Entre 11 y 50	90
d)	Más de 50	100

PROXIMA ENTREGA (Febrero 2020):

**EVALUACION DE LA GESTION DE RIESGOS EN LAS AUDITORIAS
BASADAS EN RIESGOS**