KPMG

Auditoría Interna Re Imaginada

Evolucionando para nuestros clientes

Agosto 2019

home/kpmg.co

Auditoría Interna Re Imaginada

Evolucionando para nuestros clientes

Agosto 2019

home.kpmg/co

Autores | KPMG en Colombia

Fabian Echeverría Junco
Socia Líder de Consultoría
fecheverria@kpmg.com

Claudia Patricia Contreras Ruíz
Socia Líder de IARCS[1]
cpcontreras@kpmg.com

Omar Arteaga Hernández
Director IARCS
oarteaga@kpmg.com

Víctor Adalmer Vásquez Mejía
Director ITA in Risk Consulting
vavasquez@kpmg.com

Deyanira Eliana Maritza Díaz Garzón
Gerente Senior, IARCS
ddiaz@kpmg.com

Martha Patricia Martínez Castellanos
Gerente Senior IARCS
mpmartinez@kpmg.com

Yuly Paola Muñoz Algarra
Gerente Senior IARCS
ypmunoz@kpmg.com

Marcela Ramos Parra
Gerente Senior, IARCS
marcelaramos@kpmg.com

Luz Adriana Tamayo Quintero
Gerente Senior IARCS
ltamayo@kpmg.Com

Carlos Alberto Ariza Hoyos
Gerente IARCS
cariza@kpmg.com

Leonardo Mora Daza
Gerente IARCS
leonardomora@kpmg.com

Dora Lucía Arismendi Roys
Gerente ITA in Risk Consulting
doraarismendi@kpmg.com

Diva María Guadalupe Ramírez López
Especialista en Inversiones IARCS
divaramirez@kpmg.com

Oswaldo Flórez Cortés
Supervisor Senior IARCS
oflorez@kpmg.com

Kelly Johana Piñeros
Supervisor Senior IARCS
kpineros@kpmg.com

Ivonne Eliana Barrera Valencia
Senior IARCS
ibarrera@Kpmg.com

Patricia Emilia Martínez Rodríguez
Senior IARCS
pemartinez@kpmg.com

John Alexander Piracun Bustos
Senior IARCS
jpiracun@kpmg.com

Cindy Juliana Vera Vega
Senior IARCS
cindyvera@kpmg.com

1 Servicios de Auditoría Interna, Riesgos y Cumplimiento (IARCS por sus siglas en Inglés).

Contenido

Dale clic a cualquiera de nuestros enunciados y ve directamente al contenido.

Gráficas

Tablas

Prólogo

Los puntos focales y prioridades de la función de auditoría interna enmarcan esta publicación creada para agregar valor y mejorar las operaciones de una organización, ayudando a cumplir sus objetivos a través de un enfoque inspirador, moderno y con alto nivel de liderazgo para promover cambios e innovación, no solo para la función sino para toda la organización a través de gestión de riesgos, control y gobierno.

Este documento nace a raíz de las experiencias de la práctica de Auditoría Interna de KPMG en Colombia, la cual durante los últimos 20 años ha trabajado en la construcción de un servicio de alto valor agregado tanto para entidades del sector público como privado.

A lo largo de los años, se han invertido importantes recursos a la práctica de Auditoría Interna de KPMG, enfocados en el desarrollo de auditorías internas efectivas y formación de profesionales con alto nivel de pensamiento crítico, capacidad de comunicación y mayores habilidades de relacionamiento; aspectos como estos se abordan en el libro, dando pautas y recomendaciones sobre cómo desarrollarlos en pro del crecimiento de la organización.

Se da por entendido la aplicación de un enfoque basado en riesgos en la mayoría de las funciones de auditoría interna; sin embargo, para pasar de la teoría a la práctica del enfoque de auditoria no es fácil, especialmente cuando hay cambios en el modelo operativo empresarial, un modelo digital o más conectado con los clientes, así como procesos de transformación empresarial o reorganizaciones, donde los nuevos riesgos son numerosos y se debe tener habilidad para identificarlos y asegurarlos.

Un equipo de gerencia y comité de auditoría que reconoce el apoyo y valor de la función auditoría interna es el resultado de mejoras en la proactividad, liderazgo, apalancamiento e implementación de nuevas tecnologías, mejora en las visiones futuras, prospectivas y madurez del equipo de auditoría.

Aspiramos a través de este libro hacer una invitación a la transformación de la función de auditoría interna, con el fin de seguir siendo una parte activa en el desarrollo de un modelo de gobierno, riesgos y cumplimiento evolucionado; con capacidad de respuesta a los cambiantes y nuevos retos empresariales.

Esperamos que sea de utilidad e interés para todos nuestros clientes y conocidos.

Fabian Echeverría Junco
Socio Líder Consultoría
KPMG en Colombia

Presentación

La función de auditoría interna, como tercera línea de defensa en el modelo de gobierno, riesgos y controles, debe jugar un papel preponderante en el monitoreo del negocio, como líder activo de la coordinación del aseguramiento integrado que demandan las organizaciones de hoy.

Hemos condensado en esta publicación los aspectos relevantes para que la función de auditoría interna llegue a ser ese "Socio Estratégico de Negocios" que los Presidentes del Comité de Auditoría y los Directores Financieros están reclamando por más de tres años, a fin de cerrar la brecha de valor entre lo que ellos definen como sus prioridades y lo que reciben de la auditoría interna.

Para contribuir con este desafío, el equipo gerencial y el staff de la práctica de auditoría interna de KPMG en Colombia, con la colaboración de los especialistas de ITA en Risk Consulting, a través de un trabajo minucioso y comprensivo, ha recopilado en este documento el resultado de su experiencia, agrupando en dos capítulos distintos los temas abordados; en el primero denominado "Mejorando el valor estratégico de la auditoría interna", cuyo propósito es identificar los elementos estratégicos en los cuales se espera un aporte de valor por parte de la auditoría interna e incluso se demanda que esta función integre en sus procesos y operaciones algunos de los temas allí señalados. Este capítulo incluye temáticas como la auditoría en la gestión de gobierno, riesgos, cumplimiento, expectativas sobre la generación de valor de la auditoría interna, el papel de la auditoría en la gestión de riesgos emergentes, Data & Analytics como habilitador principal de la función de auditoría interna, el pensamiento crítico y lo que se espera de los auditores internos.

En el segundo capítulo denominado "Auditoría Interna de Valor", hemos condensado temas relevantes para ayudar a los equipos de auditoría interna en la planeación y ejecución de auditorías eficientes y efectivas, sobre temas específicos y muchas veces estratégicos de los negocios para los cuales sirven como función y por ende hacen parte del universo de auditoría y deben ser considerados en el plan de auditoría, cualquiera que sea su horizonte en el tiempo.

Con ello se pretende ofrecer ideas para los auditores internos, de manera que puedan planear y generar resultados de impacto y con alto contenido técnico, considerando el acompañamiento de especialistas para cada tema. Lo primero es comenzar por tocar el tema de la transformación de la función de auditoría interna, partiendo nuevamente de la necesidad de evolucionar el pensamiento tanto de los auditores internos como de la Alta Dirección, en el sentido de entender que el verdadero valor de la auditoría interna se da cuando se abren espacios de participación de esta función, en la Junta Directiva, Consejo Directivo, Consejo de Administración o cualquier otro estamento directivo y estratégico, para que puedan aportar sus conocimientos en las estrategias de transformación y crecimiento de la organización a la que sirven, dado que su enfoque moderno no es policivo sino asesor, tal como lo establece la definición de auditoría interna del Instituto de Auditores Internos que dice "La 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 riesgos, control y gobierno."

En este capítulo se incluyen temas como auditoría a la gestión integral de riesgos, y en especial a la cultura organizacional frente al riesgo, auditoría a la gestión de riesgos en salud, auditoría en el sector de pensiones, auditoría de inversiones, auditoría externa de gestión y resultados, auditoría interna en la evaluación de riesgos de ciberseguridad, auditoría en cloud computing, riesgos asociados a la integración del Blockchain y auditoría de tecnologías de información.

Nuestra ambición es que esta publicación sea de valor y utilidad para que los auditores internos encuentren en ella apoyo y consejos prácticos para mejorar su desempeño y lograr su objetivo estratégico de ser el aliado de la alta dirección en la transformación de su negocio, integrando en su quehacer y en sus auditorías, la competencia y la capacidad para evaluar las tecnologías disruptivas que den sentido y hagan tangible el valor agregado que se espera de esta importante función en el engranaje de la organización.

Claudia Patricia Contreras Ruíz
Socia Líder de IARCS
KPMG en Colombia

1. Mejorando el valor estratégico de la auditoría interna

1.1 La auditoría en la gestión de gobierno, riesgo y cumplimiento

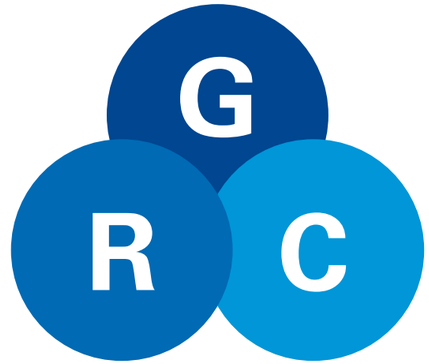
Gobierno, Riesgo y Cumplimiento (GRC) aún es un modelo holístico naciente en las organizaciones, que ha venido evolucionando frente a la materialización de riesgos, fraudes, incidentes de seguridad cibernética y penalizaciones por ausencia de controles de la operación frente a los exigidos por los reguladores.

Los retos de la globalización demandan una mayor capacidad de adaptación de las organizaciones ante las grandes transformaciones, las tecnologías, las exigencias de un mercado, así como la cooperación global para que obtengan un crecimiento sostenible en el tiempo, las han enfrentado a la materialización de las situaciones mencionadas anteriormente.

Uno de los retos más importantes de las Juntas Directivas es que las organizaciones gocen de estándares de gobierno corporativo, donde exista presencia de miembros independientes que puedan controvertir a la administración con su conocimiento y experiencia, gestionando de manera efectiva los riesgos y asegurando el cumplimiento regulatorio. Las Juntas Directivas deben determinar los perfiles de sus miembros, de acuerdo a las necesidades del negocio, identificar cuáles son las responsabilidades de sus miembros, tener mecanismos y herramientas adecuadas de evaluación interna y externa, comités de apoyo y reglamentos estrictos.

> El máximo órgano de la dirección, la junta directiva, representantes legales, administradores, auditor interno, revisor fiscal, órganos de control, y otros grupos de interés, necesitan ver cómo van las cosas en la organización, para estar involucrados en lo que ocurre y en lo que sucederá en el futuro, de tal manera que estén alineados para tomar mejores decisiones, dando seguimiento a la acción del gerente general, y presionando para tener un plan táctico que dé resultados efectivos. De esta manera, la información fluye de arriba hacia abajo, y viceversa. KPMG define el GRC como un enfoque **para alinear los procesos de gobierno, riesgo y cumplimiento de la organización con su estrategia**, lo que permite la convergencia y la transparencia de la información para impulsar el rendimiento y la resiliencia en un entorno empresarial económico dinámico. En la gráfica 1, se relacionan los componentes relevantes por cada uno de los procesos.

Gráfica 1. Componentes relevantes en cada proceso



Gobierno

- Estrategia
- Misión y visión
- Roles y responsabilidades
- Políticas y procedimientos (internos y externos)
- Estructura y procesos
- Propiedad establecida, responsabilidad y comunicación
- Activos de información

Administración de riesgos

- Apetito de riesgo
- Identificación del riesgo
- Evaluación del riego
- Perfiles de riesgos
- Indicadores claves de riesgos (KRIs)
- Análisis de riesgos
- Riesgos agregados
- Eventos de pérdida
- Excepción / problemas y seguimiento de aceptación de riesgos
- Propiedad y comunicación de riesgos

Cumplimiento

- Identificación del marco normativo
- Identificación de controles
- Pruebas de diseño y efectividad operativa
- Excepciones / seguimiento de problemas
- Análisis de causa raíz
- Seguimiento a planes o esfuerzos de remediación
- Auditoría / monitoreo continuo
- Propiedad y comunicación de actividades de control y brechas

Estas actividades integradas en un
Programa GRC holístico
puede ser habilitado por un **GRC Tecnológico Empresarial.**

Fuente: Metodología KPMG – Government, Risk & Compliance (GRC)

Gobierno

El gobierno corporativo provee un marco que define derechos y responsabilidades, dentro del cual interactúan los órganos de gobierno de una organización. Este sistema obedece a principios universales, siendo distinto y único para adaptarse a la singularidad de cada organización y al nivel de madurez que hayan alcanzado las prácticas de su alta dirección; es por esto, que al implementar un modelo formal y evolucionado de gobierno corporativo, se considera la calidad de su administración y los compromisos que sus directivos están dispuestos a realizar; de esa forma, la estructura del gobierno podrá generar valor para el negocio, al considerar:

- El marco eficaz para el gobierno corporativo: disposiciones legales y reglamentarias, cultura financiera, incentivos, entre otros elementos.
- El ejercicio de derechos y funciones de los accionistas.
- Tratamiento equitativo de los accionistas (mayoritarios y minoritarios, nacionales y extranjeros).
- Papel de las partes interesadas: empleados, clientes, proveedores, la comunidad, entre otros.
- Revelación de información y transparencia.
- Responsabilidad de la Junta Directiva, especialmente en lo referido al direccionamiento estratégico, al control efectivo de la dirección ejecutiva y a la protección de los intereses de los accionistas.

Un adecuado gobierno corporativo, pretende evitar malas prácticas administrativas, dificultades en los cambios de cultura y generar credibilidad en el negocio; su propósito es:

- Generar confianza en los inversionistas y mercados, mejorando el flujo de información desde y hacia la organización.
- Institucionalizar mejores prácticas en cuanto a transparencia, resolución de conflictos y toma de decisiones.
- Proteger la propiedad y los intereses de accionistas, implementar mejores prácticas de estándares éticos y acciones de responsabilidad operativa.

Riesgo

Las organizaciones están expuestas a diversos riesgos que pueden comprometer su crecimiento, poner en entredicho la viabilidad del negocio, desacelerar su crecimiento y posicionamiento en el mercado. Para responder apropiadamente frente a estos riesgos, las organizaciones deben contar con metodologías de gestión de riesgo y marcos de control, apoyados en herramientas tecnológicas que soporten los procesos y procedimientos de monitoreo y revisión de cumplimiento, permitiendo que el negocio opere de forma preventiva ante pérdidas económicas que impacten a la organización.

La encuesta de GRC - Gestionando el control[2] reveló que 91% de los encuestados reconocen haber enfrentado la materialización de algún riesgo durante los últimos meses anteriores a esta, una cifra importante a tener en cuenta por quienes aún carecen de un modelo de defensa robusto que les permita identificar y administrar riesgos de forma rápida, mejorar el ambiente de control de los procesos dentro la organización y gestionar de manera preventiva riesgos que puedan afectar significativamente a la organización. Entre los riesgos más relevantes que se han materializado, según la encuesta realizada están:

- Fraude por parte de proveedores, empleados o clientes.
- Conflictos de segregación de funciones.
- Violación a las políticas o reglas de negocio.
- Conflicto de interés.
- Robo de activos físicos e información.
- Pérdida de información.
- Falta de integridad de la información.
- Incumplimiento a leyes gubernamentales o regulaciones.
- Daño reputacional.
- Penalizaciones en contrato por incumplimiento.

A menudo, las funciones de control frente a sus riesgos operan en silos[3] no comunicados, lo que puede generar diferentes definiciones del término de gestión de riesgos en instrucciones y directrices, opiniones encontradas sobre riesgos y prevención, duplicidad o brechas en la cobertura grupal, diferentes estructuras, períodos y formatos para reportar, diferentes roles y responsabilidades, procesos no formalizados, así como duplicar los esfuerzos de gestión de riesgos por unidades de negocio.

Por lo anterior, es importante que las organizaciones que hayan definido e implementado su sistema de administración de riesgos evalúen su nivel de madurez para determinar el grado de confianza que puede dárseles y generar recomendaciones para optimizarlas; en la gráfica 2 se presentan las funciones a considerar para realizar una evaluación del nivel de madurez del sistema de administración de riesgos que le permitirá focalizar los esfuerzos del plan de auditoría interna.

2 Encuesta de Gobierno, Riesgo y Cumplimiento- Gestionando el Control, KPMG México, 2018

3 Incapacidad para trabajar eficientemente entre áreas o unidades de negocio.

Gráfica 2. Funciones del sistema de administración de riesgos

Fuente: Metodología KPMG – Enterprise, Risk Management (ERM)

Cumplimiento

El objetivo de la estrategia de cumplimiento, es evitar o minimizar los riesgos de multas, reputacionales, operativos y financieros. A largo plazo la estrategia de cumplimiento se incorpora como una parte sustancial de la estrategia comercial y de riesgos, existiendo una fuerte conectividad de las funciones legales y de cumplimiento con la organización.

El marco de cumplimiento normativo debe considerar la identificación de las leyes, normas y políticas. Los riesgos más complejos, el mayor control regulatorio y un entorno de cumplimiento más riguroso han aumentado significativamente los desafíos para la gestión de riesgos y cumplimiento en las organizaciones. Debe ser claro para las organizaciones que el cumplimiento se extiende a través de múltiples ubicaciones, por tanto se requiere de un conocimiento profundo de la organización, de su entorno económico, la normatividad local e internacional que le aplique según su objetivo de negocio, los requerimientos regulatorios, los cambios en sus estructuras y demás elementos que puedan afectarle. En la gráfica 3 se establecen, pero no se limitan, los elementos que debería considerar una organización en la definición de la estrategia de cumplimiento.

Gráfica 3- Elementos a considerar para establecer el marco de cumplimiento

Fuente: KPMG construcción propia.

La auditoría y su enfoque de valor

La auditoría interna como tercera línea de defensa, supervisa el cumplimiento de las regulaciones externas, así como las políticas y directrices internas controla la idoneidad y la solidez del marco de riesgo y cumplimiento. El gobierno corporativo a nivel de la Junta Directiva debe evaluar ciertos elementos y la auditoría interna debe verificar esos elementos. Las áreas de auditoría sugeridas incluyen:

1. Supervisión de la Junta

a. Cumplimiento de las leyes y regulaciones: la Junta Directiva debe tener un tamaño suficiente para que las habilidades y experiencia de sus miembros sean adecuadas para las necesidades del negocio.
b. Definición de independencia: los consejos de administración efectivos ejercen un juicio independiente al llevar a cabo sus responsabilidades. Requerir una mayoría de directores independientes aumentará la calidad de la supervisión de la Junta y disminuirá la posibilidad de dañar los conflictos de intereses.
c. CEO - Presidencia: los roles de presidente y CEO están separados y el presidente de la Junta es un director independiente.
d. Compromiso de tiempo: se definen y evalúan regularmente.
e. Adecuado conjunto de habilidades de la Junta: los directores miembros de la Junta son evaluados sobre las competencias definidas y las habilidades necesarias.
f. Operaciones de la Junta: las reuniones de la Junta se llevan a cabo regularmente, la información de la reunión se proporciona con anticipación, las agendas las determina el presidente de la Junta. A su vez, la Junta realiza actividades de monitoreo, educa y forma a sus miembros.
g. Principios y valores de la Junta: se define un Código de Conducta, se capacita a los nuevos miembros y se mantiene la independencia.

2. Seguimiento y evaluación del desempeño

a. Evaluación del desempeño: se ha implementado un proceso para realizar una evaluación anual.
b. Marco de remuneración: se ha establecido un comité de remuneración y un marco de referencia.
c. Formulación de la estrategia: existe una visión y una misión claras, así como una estrategia definida que está alineada con el plan de negocios. La estrategia debe incluir los aportes de la Junta Directiva y las expectativas validadas.
d. Delegación: los roles / responsabilidades, la estructura de la organización, la gestión del desempeño, los planes de sucesión y la estrategia de recursos humanos están claramente definidos.
e. Monitoreo: existe un proceso para informar sobre el despliegue de la estrategia, la Junta recibe reportes de información periódicos sobre las operaciones, hay un sistema y procesos de informes financieros sólidos, hay una comunicación rápida de errores y existe un sistema de gestión de calidad robusto.
f. Medición de resultados: los indicadores clave de rendimiento se desarrollan y utilizan para medir el rendimiento de la empresa, su administración e incluso la Junta Directiva.

3. Responsabilidad y auditoría

a. Responsabilidad: existe una política definida de denunciantes.
b. Comité de auditoría: se ha establecido un comité de auditoría, se abordan las calificaciones de auditoría, el comité se reúne con auditores internos y externos, y tiene el poder de abordar y evaluar.
c. Gestión de riesgos: la Junta Directiva supervisa la gestión de riesgos, existe un plan de continuidad empresarial y un plan de gestión de crisis, y el riesgo de fraude, mercado y proveedores se gestiona de forma proactiva.
d. Procesos: existe un ambiente que promueva el comportamiento ético (por ejemplo, el Código de conducta), existen procedimientos y marcos para las actividades principales y de apoyo, se implementa la segregación de funciones, se comunican las políticas a las partes externas y se implementan controles internos.

1.2 Expectativas sobre la generación de valor por parte de la auditoría interna

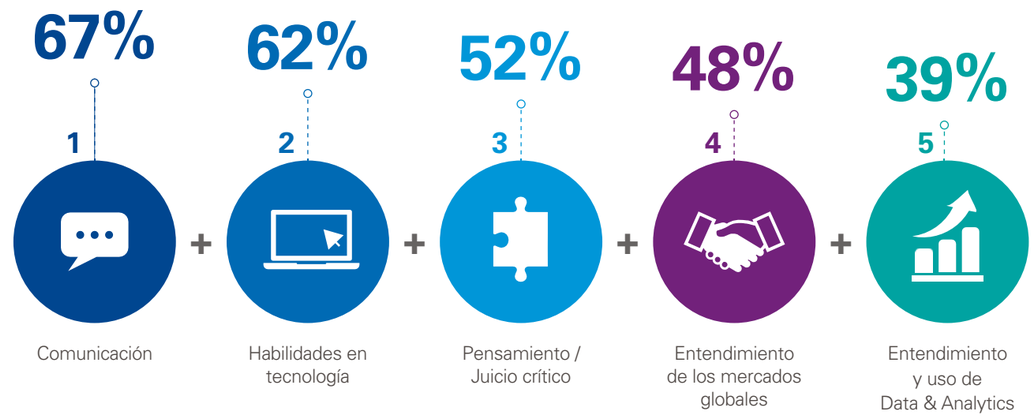
La visión y el alcance de la auditoría interna (AI), juegan un rol muy importante a la hora de generar mayor confianza en las organizaciones, ya que tiene como reto cambiar y evolucionar hacia un modelo más moderno acorde con los nuevos tiempos y capaz de responder a los desafíos del mundo globalizado. Para esto, la función de auditoría interna incluirá dentro de sus procesos el análisis de los riesgos logrando posicionarse como asesores del negocio, permitiendo impulsar iniciativas para el crecimiento y desarrollo de las entidades. Esto se puede realizar, por medio de propuestas encaminadas hacia la efectividad de los procesos y la adecuada administración de los riesgos. Adicionalmente, la auditoría interna debe contar con perfiles profesionales multidisciplinarios con competencias técnicas y habilidades necesarias para contribuir con la generación de valor teniendo claridad en el funcionamiento del negocio, así como sus objetivos y prioridades.

La auditoría interna ha desarrollado tradicionalmente un papel de verificación de operaciones con un enfoque en las actividades ejecutadas en el pasado, identificando hallazgos sobre los cuales la empresa puede ya tener conocimiento. Esta situación ha venido cambiando para ofrecer valor a la empresa, debido a que en la actualidad la AI busca hacer más auditorías predictivas, que aporten ideas y propuestas innovadoras para mejorar los procesos y que a su vez sean capaces de prevenir riesgos emergentes, esto se evidencia cuando la AI da recomendaciones que permiten disminuir los costos o incrementar las utilidades. Con el paso del tiempo la auditoría se ha volcado a alinear sus trabajos hacia los objetivos estrategicos de las organizaciones asumiendo de esta manera un rol más colaborativo manteniendo en paralelo su función de independencia. Esta evolución en el tiempo ha permitido actuar de forma más rápida y eficiente a los cambios del mercado, apoyando de esta manera la gestión de los riesgos, los impactos económicos y reputacionales.

Para lograr valor en la auditoría, los auditores deben contar con las siguientes habilidades:

1. Comunicación: comunicar de forma clara y concisa las situaciones identificadas resultado de las auditorías ejecutadas a la alta dirección y a los dueños de procesos,

Gráfica 4 Habilidades del equipo de apoyo de AI



Fuente: KPMG construcción propia artículo "Un Aliado en la Generación de Valor"

permitiendo el entendimiento de los asuntos relevantes y trabajando en conjunto para definir las acciones a tomar.

2. Expertiz tecnológico: experiencia utilizando las diferentes herramientas tecnológicas para poder realizar diferentes tipos de pruebas tanto en auditorías tecnológicas como de procesos, lo que permita identificar aspectos que antes no habían sido monitoreados logrando así optimizar los recursos y generar mayor productividad en los diferentes procesos.
3. Pensamiento crítico: aptitudes y actitudes que ayuden a emitir juicios sobre los procesos evaluados; decir que el auditor debe contar o desarrollar pensamientos y respuestas lógicas para debatir los resultados y soportes encontrados.
4. Entendimiento de los mercados globales: el auditor debe conocer y estudiar los mercados existentes y nacientes para formar un criterio válido de evaluación que permita generar auditorías basadas en hechos y buenas prácticas del core de negocio.
5. Entendimiento y uso de Data & Analytics: conocer las herramientas y procedimientos para el análisis de datos, permite que el auditor no se enfoque en muestras sino tenga la posibilidad de analizar toda la información y enfocarse en aquellos aspectos que se salen de la norma, permitiendo a los auditores prevenir riesgos futuros de manera eficiente y productiva y en lo posible proyectar con precisión el impacto que estos tendrán.

De acuerdo a lo anterior, en la gráfica 4 se relacionan las habilidades que deben tener los auditores para posicionarse como un punto de apoyo visto desde la alta gerencia, y que pueden generar un beneficio en los resultados suministrados a las entidades.

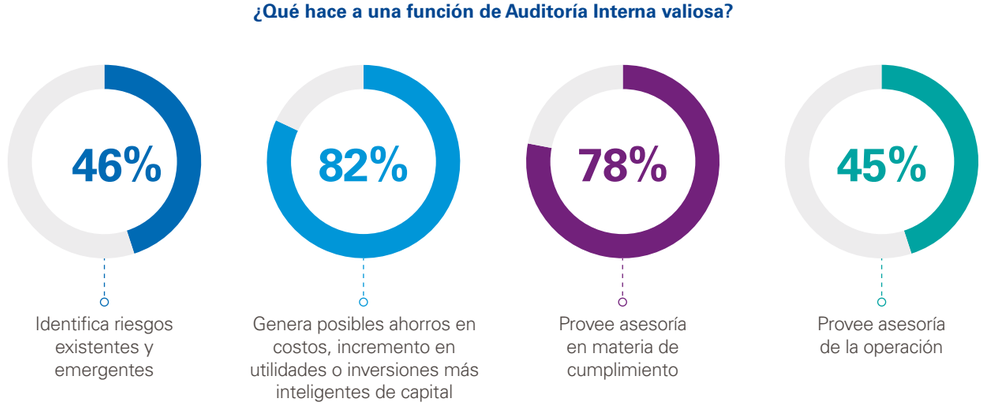
Los auditores que logran mejorar sus competencias convierten su rol en apoyo y confianza, impulsando a que las entidades sientan la necesidad de contar con una auditoría como base para un adecuado modelo de buen gobierno corporativo y aseguramiento de la efectividad de los controles.

La AI se relaciona con todas las áreas de una compañía a fin de contribuir con los objetivos de las organizaciones para el cumplimiento de sus metas, sin perder su independencia y objetividad. También es importante resaltar que para cumplir con el propósito de generar valor agregado por parte del área de AI es importante que los auditores entiendan los objetivos comerciales de las organizaciones, identificar los riesgos más significativos a fin de enfocar sus esfuerzos en las áreas donde se puede agregar mayor valor.

Objetivos claves de la auditoría interna para aportar valor en las organizaciones

Hablar de objetivos claves de la AI no es simple, pues conceptualmente éstos van ligados al perfil y estrategias de cada organización. Debido a esto es esencial que los componentes del plan de AI se establezcan buscando la optimización y potencialización de los procesos a lo largo de

Gráfica 5 Aspectos relevantes para generar una auditoría de valor



Fuente: Seeking value through Internal Audit, KPMG International Forbes, 2016.

toda la cadena de valor. De esta manera la AI asume un papel estratégico en las compañías convirtiéndolos en un asesor de confianza para la alta dirección, mostrando cambios hacia la generación de ahorros en costos, incremento de utilidad o inversiones más inteligentes, permitiendo identificar riesgos existentes y emergentes y proporcionando asesorías en materia de cumplimiento y de la operación.[4]

Para que las áreas de AI logren aportar valor a las diferentes organizaciones es importante que en esta trasformación tengan en cuenta los siguientes pilares:

1. Mejorar la estrategia de auditoría interna mediante visión de riesgo única y trabajo coordinado con otras áreas "Aseguramiento Integrado".
2. Nuevas variables y madurez de los sistemas de Administración de Riesgos para focalizar esfuerzos de auditoría.
3. Data Analytics, Robotics Process Automation, Cognitive Technology para habilitar la auditoría interna.
4. Eficiencias para monitorear el universo de controles (Control Self Assessment – Costeo)

En el contexto globalizado de hoy la AI es un componente de aseguramiento de calidad de la información, lo cual contribuye a la eficiencia de los procesos de control interno, gestión de riesgo y gobierno. El valor agregado de AI se basa en los pilares fundamentales para asumir el nuevo esquema el cual sigue siendo un reto y un desafío para cualquier departamento de AI a nivel mundial.

La utilización de herramientas tecnológicas permite analizar con mayor confiabilidad la información, brindando la oportunidad de diseñar indicadores de monitoreo continuo que facilitan el seguimiento a la auditoría, generando impacto y beneficio a la compañía en prevención de riesgos y ofreciendo información adecuada y oportuna para la toma de decisiones.

El departamento de AI debe contar con un equipo multidisciplinario con diversos perfiles profesionales a fin de convertirse en un asesor de negocio para la Alta Dirección de las organizaciones.

4 Basado en un artículo de KPMG "Un Aliado en la Generación de Valor", por Juan Carlos Reséndiz.

1.3 El papel de la auditoría en la gestión de riesgos emergentes

Los riesgos emergentes y su tendencia

En un mundo donde la evolución es una constante dinámica, asociada a los avances tecnológicos, cambios socioeconómicos, climáticos, demográficos, geopolíticos, culturales, normativos, tendencias de globalización, medioambientalistas y de sostenibilidad (gráfica 6), las organizaciones se han visto en la necesidad de adaptarse e innovar para poder responder ante los riesgos emergentes, los cuales se caracterizan por:

- Tener una velocidad, persistencia, probabilidad de ocurrencia e impacto difícil de evaluar, lo cual hace compleja su identificación y cuantificación.
- Un alto nivel de incertidumbre debido a la poca información que puede existir sobre ellos.
- Sus causas y consecuencias pueden ser ambiguas.
- Son pocas las entidades que se arriesgan a ser los primeros en abordarlos.

Dado lo anterior, se considera que estos riesgos no pueden ser controlados, sino que solo se puede mitigar la exposición a los mismos. Sin embargo, los efectos de los riesgos emergentes en una organización pueden llegar a convertirse en una oportunidad de negocio o por el contrario ser un factor que amenace el cumplimiento de los objetivos estratégicos. Siendo importante que los auditores realicen las siguientes preguntas con el fin de poder enfocar de forma adecuada su plan de trabajo, ¿es consciente la organización de sus riesgos emergentes?, ¿cómo podemos apoyar y orientar su identificación?.

Teniendo en cuenta el contexto Latinoamericano, según el reporte "III Benchmark de Gestión de Riesgos en Latinoamérica" realizado en el 2018 por Marsh Risk Consulting y RIMS[5], una de cada dos empresas (50%) valora los riesgos emergentes, el 45% de organizaciones dicen no hacerlo y el 5% manifiesta no conocer este tipo de riesgos; en cuanto a las industrias se destaca la gestión de riesgos en Petróleo y Gas, Energía y Servicios Públicos, Transporte, Construcción e Infraestructura, e Instituciones Financieras. En el caso colombiano, el reporte indica que ocupa el tercer lugar con el 54,7% de organizaciones que contemplan y gestionan los riesgos emergentes y un 45,3% mencionan no conocer sobre estos.

5 Marsh Risk Consulting; RIMS. (Enero de 2018). Tomado de Marsh LLC: https://www.marsh.com/co/insights/research/iii-benchmark-de-gestion-de-riesgos-en-latinoamerica.html

De igual forma, describen las principales fuentes de información a la hora de la identificación y análisis de estos riesgos, entre las que se destacan noticias y publicaciones de industria, análisis interno y externo de la información de la compañía y conocimiento aportado por los miembros de la alta gerencia. En el caso de las noticias y publicaciones entre mayor sea el volumen de documentos consultados mayor será la información y el contexto que se tenga acerca de un tema en particular, permitiendo conocer su perspectiva desde otros puntos de vista. En cuanto al análisis interno y externo de información, este debe estar soportado en datos internos de las compañías los cuales se basan en hechos reales o información externa obtenida desde el enfoque de las auditorías o consultorías especializadas. Por último, la información aportada por los miembros de la alta gerencia, es adquirida a partir de la experiencia y conocimiento de estos en el sector, la empresa, sus procesos y las tendencias de la industria, la economía y el entorno en general.

Gráfica 6 Principales factores de los riesgos emergentes

Fuente: KPMG - Factores de riesgos emergentes

No obstante, son diversas las fuentes de información y perspectivas que se pueden tener en cuenta, tal como se muestra en la gráfica 7, por lo que adicional a las mencionadas, también se pueden tener en consideración los siguientes aspectos:

- Estudios macroeconómicos y microeconómicos que pueden afectar la industria
- Los riesgos internos de la compañía
- Problemas y/o potenciales cambios en la industria
- Desafíos estratégicos y nuevos proyectos
- Posibles cambios regulatorios

Aunque actualmente no existe una metodología específica que permita asegurar la identificación de los riesgos emergentes, desde la perspectiva de la auditoría se considera y se resalta la importancia de los siguientes pasos en la identificación y gestión de riesgos emergentes, los cuales contemplan la identificación y análisis de factores internos y externos, evaluación y priorización, definición de indicadores y mecanismos de medición, análisis de escenario y determinación de partes afectadas y partes responsables en su gestión. En la gráfica 8, se relacionan los pasos para la identificación de riesgos emergentes:

Gráfica 7. Fuentes de información para identificar y entender los impactos potenciales de los riesgos emergentes

Fuente: "III Benchmark de Gestión de Riesgos en Latinoamérica" publicado por Marsh Risk Consulting; RIMS

Gráfica 8. Pasos para la identificación y gestión de riesgos emergentes

Fuente: KPMG construcción propia

Apoyo de la auditoría en la gestión de riesgos emergentes

A nivel general, el enfoque de la auditoría interna tiende a estar orientado en evaluaciones de cumplimiento, identificación de amenazas de riesgo y eventos ya materializados, los cuales en el mejor de los casos ya han sido identificados y gestionados por las compañías y éste debe cambiar, desde la auditoría se debe propender por incluir la identificación y evaluación de riesgos emergentes a partir del desarrollo de la visión, análisis y anticipación de eventos futuros, lo que permitiría el incremento del valor para las organizaciones, según lo sugerido por el Presidente y Director General del Instituto de Auditores Internos en el artículo "Auditoria interna y Riesgos Emergentes desde la cima de la colina al escritorio"[6]. De igual forma, indica que las mejores funciones de auditoría interna del mundo se encuentran preparadas para centrarse en el futuro, manteniendo la agilidad e identificando y abordando de forma proactiva los riesgos emergentes, labor que se debe realizar de forma conjunta con la administración.

Con el fin que los auditores puedan brindar un mayor apoyo a las organizaciones en la identificación de riesgos emergentes, teniendo en cuenta que entre las principales fuentes de información se encuentra la obtenida por la alta gerencia, Gartner[7] o consultó a más de 200 directores ejecutivos de auditoría y estableció para el 2019, riesgos clave agrupados en cuatro temas principales, los cuales se encuentran en gran medida asociados a factores emergentes y pueden brindar tanto a la auditoría como a las compañías una visión más amplia para la identificación y gestión de los mismos.

Gráfica 9. Riesgos clave para el 2019

Fuente: KPMG, 11 riesgos clave para el 2019 que todo auditor debe conocer

Frente a estos grupos de riesgos, cabe destacar:

a. En el entorno actual los datos generados por las organizaciones han tomado un papel significativo como base para la toma de decisiones y establecimiento de la estrategia corporativa, pero el aseguramiento de su calidad, protección y uso responsable se torna complejo ante las actualizaciones y avances tecnológicos que se presentan día a día; por esto se deben establecer las políticas y lineamientos necesarios para la gobernabilidad de datos y establecer mecanismos de control y seguimiento adecuados que permitan asegurar su efectividad.

b. Debido a la dependencia de las organizaciones en el uso de las nuevas tecnologías para su crecimiento y sostenibilidad, éstas se ven en la necesidad de innovar y estar a la vanguardia para ajustarse a los constantes cambios y responder oportunamente a las vulnerabilidades que esto implica; por lo que el establecimiento y la evaluación de los controles generales de tecnología de la información (TI) cobran mayor relevancia y es vital contemplarlos en el plan de auditoría.

c. La existencia de altos niveles de competitividad lleva a las organizaciones a innovar e invertir en proyectos de transformación digital con el fin de expandirse a nuevos sectores y mercados, para mantener la eficiencia de los costos se deben ajustar al ritmo de los mercados e incluso ajustar la planificación estratégica de la fuerza laboral para poder contar con personal técnico que se adapte y responda eficientemente ante estos cambios y los riesgos que implican; en este sentido desde la auditoría se debe asegurar una adecuada gestión de proyectos, la cual debe estar alineada frente a la estrategia corporativa y en cumplimiento con los lineamientos y objetivos propuestos al interior de la compañía.

d. Se destaca el alto y creciente nivel de incertidumbre y volatilidad a nivel político, económico, legal, y los desafíos globales que implica la gestión actual de los negocios, lo que dificulta el establecimiento de la estrategia corporativa a largo plazo y el diseño de planes de acción apropiados que permitan asegurar de forma razonable su cumplimiento y sostenibilidad. De esta forma, es importante contemplar la auditoría de riesgos estratégicos, incluyendo análisis de escenarios, ajuste del apetito de riesgo, planes de acción y de contingencia que permitan a las organizaciones mitigar y/o recuperarse de forma eficiente frente a una posible crisis.

Lo anterior, invita a los auditores a cambiar su enfoque detectivo, de control y cumplimiento, por un enfoque más analítico, preventivo, innovador y adaptable ante el dinamismo de la sociedad actual, los negocios, sus estrategias y las expectativas de los diversos grupos de interés, lo que permitiría obtener un mayor nivel de credibilidad para las funciones de auditoría y convertirlas en un aliado estratégico para la generación de valor en las organizaciones, convirtiendo los riesgos en oportunidades.

6 Chambers, R. F. (Agosto de 2018). The Institute of Internal Auditors. Obtenido de Auditoría interna y Riesgos Emergentes: desde la cima de la colina al escritorio: https://global.theiia.org/knowledge/chambers-spanish/Pages/Auditoria-interna-y-Riesgos-Emergentes-desde-la-cima-de-la-colina-al-escritorio.aspx

7 Gartner´s Malcom Murray, Rafael go and Leslee Mcknight, 2019.

1.4 Data & Analytics en la auditoría interna.

La función de auditoría interna se enfrenta a grandes retos actuales, todos ellos encaminados a la creciente demanda de requerimientos y expectativas de los diferentes stakeholders de las organizaciones, quienes sienten que existe una 'Brecha de Valor ' entre lo que tienen definido como prioridades y lo que reciben de sus funciones de las áreas de auditoría.

Es por ello que el desempeño de la función de auditoría debe ir evolucionando su nivel de madurez (Gráfico 10), estableciendo acciones que le permitan pasar de un nivel tradicional – mejorado a un estado avanzado, en donde su visión de aseguramiento integre la disponibilidad de la tecnología para una sola visión de riesgos, control y monitoreo, que le apoye en focalizarse en áreas y aspectos de mayor impacto para la organización, contribuyendo al logro de los objetivos estratégicos de la misma.

¿Qué beneficios trae consigo la evolución del nivel de madurez de la Función de Auditoría Interna?

- Una función de auditoría interna que efectivamente pueda tener un impacto notable y añadir valor a través de la organización.
- Un desempeño de función más eficiente y eficaz orientado al análisis de los datos.
- Una función de auditoría interna bien desarrollada y alineada que proporcione un recurso y una oportunidad importante para la organización de precisar sus controles, reducir los riesgos, identificar posibles eficiencias requeridas y direccionar beneficios en costos.

Gráfica 10. Nivel de madurez de la función de auditoría

	- Tradicional -	- Mejorado -	Integrado — Estado futuro
	Tradicional (Básico)	**Mejorado (Intermedio)**	**Integrado (Avanzado)**
Evaluación de riesgo	• Hallazgos previos de auditoría. • Enfoque en riesgos financieros.	• Evaluación anual de riesgo AI. • Considerar perfil ERM. • Alineación de las definiciones de riesgo y criterio a través de funciones de aseguramiento.	• Visión, asesoramiento y aseguramiento objetivo basado en riesgos. • Identificación proactiva de riesgos. • Identificación y valoración de riesgos integradas. • Monitoreo del riesgo en tiempo real.
Nivel de aseguramiento	• Coordinación limitada en la cobertura de riesgos. • Centrada en la detección de problemas y errores. • Enfocadas en control operacional (políticas y procedimientos) y cumplimiento normativo.	• Apalancamiento de la documentación soporte de aseguramiento. • Coordinación del cubrimiento de riesgo.	• Grupos de aseguramiento y Auditoría Interna coordinan la cobertura de riesgos. • Coordinación de pruebas (Pruebas multi propósito). • Análisis definido para perfeccionar la cobertura de riesgos por función. • Evolución del plan de auditoria de manera dinámica.
Desarrollo del plan de auditoría interna	• Identificación de auditorías con enfoque cualitativo. • Entidades tradicionales auditables.	• Incorporación de mediciones cuantitativas y cualitativas, por ejemplo; tendencias de los estados financieros y KPIs.	• Disponibilidad de la tecnología para una sola visión de los riesgos, controles y monitoreo. • Foco en áreas de riesgo emergente, cultura, ciberseguridad, fraude, móviles, redes sociales, etc. • Uso de variedad de técnicas de auditoría incluyendo revisiones de extremo a extremo, auditorías de gobierno, participación en proyectos, revisiones de pre-implementación, etc.
Ejecución auditoría interna	• Entendimientos basados en indagación. • Hallazgos y oportunidades de mejora son identificados por documentación formal.	• Análisis de datos/ uso de tecnología. • Combinación de técnicas de auditoría y áreas de enfoque.	

Así como un departamento de Auditoría Interna madura y evoluciona para informar y afectar el negocio más positivamente, este refinará la forma en que desarrolla, actualiza y evalúa continuamente el riesgo, como soporta y se alinea con otras áreas de aseguramiento, y como prueba y monitorea el negocio.

Fuente: KPMG – Auditoría Interna del Futuro

Fortalecimiento de la estrategia de la auditoría interna hacia la revolución de los datos

Un elemento fundamental a considerar como parte de esta evolución, en la revolución de la función de la auditoría interna es el direccionamiento de los datos – Data Analytics - como parte de la estrategia de auditoría interna; según el Instituto de Auditores Internos en su artículo "*Perspectivas y Visiones Globales*" ,"*Los análisis de los datos proporcionan a los auditores internos la capacidad para analizar las poblaciones totales y posibles correlaciones, mejorando así la capacidad de aseguramiento y la oportunidad de proporcionar visión y previsión*". Este direccionamiento hacia datos, permitirá:

- Cambiar muchos hallazgos no relevantes a menos hallazgos pero de mayor impacto.
- Cambiar un enfoque de revisión de actividades pasadas o investigar hechos cumplidos e involucrar una mirada hacia adelante.
- Proveer mayor valor en el análisis de los procesos que contribuya al monitoreo y/o mitigación de riesgos, a través de tableros de aseguramiento o como habilitador de la auditoría.
- Construcción de indicadores para medir la efectividad de los controles.

Desafíos con el uso de data analytics

Como habilitador de la auditoría

Uno de los desafíos a los que nos enfrentamos en todo este proceso de cambio, es el uso de la data durante la ejecución del plan de auditoría, para lo cual es importante considerar:

- El entendimiento del flujo de la información del proceso objeto de auditoría y riesgos asociados.
- Conocimiento de la data del proceso objeto de auditoría en asociación con sus normas, políticas y procedimientos.
- Análisis de la data con herramientas de inteligencia de negocios como por ejemplo Power BI, Qlick, Tableu, entre otros.
- Direccionamiento del plan de pruebas hacia la identificación de excepciones y posible materialización de riesgos de proceso y riesgos ocultos en la data.

De esta forma podremos decir, que con data analytics se habilitó el desarrollo de una auditoría focalizada, de impacto y basada en riesgos.

Data Analytics de habilitador de la auditoría al monitoreo continuo

Con el uso de los datos se puede responder de una manera importante y notable a las expectativas de los stakeholders de las organizaciones, pasando del aseguramiento de riesgos hacia la prevención de su materialización, bajo un monitoreo continuo a través de tableros de control.

El diseño y gestión de estos tableros de control, permitirá al auditor:

- Identificar los riesgos a monitorear a través de indicadores.
- Actualizar automáticamente los datos que permiten identificar alertas tempranas.
- Evaluar el 100% de la información.
- Generar valor agregado en la toma de decisiones, logrando identificar posibles nuevos riesgos y la creación de nuevos controles.
- Mejorar la forma de auditar los procesos.
- Contribuir en el fortalecimiento de la gestión de los procesos auditados.

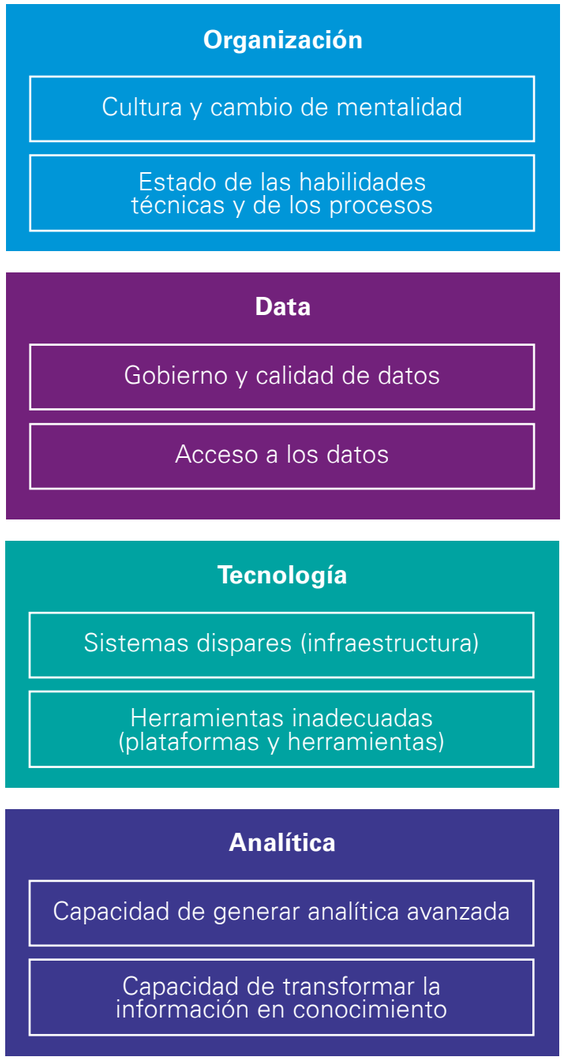
Es importante resaltar, que el diseño de estos tableros de control, también puede contribuir a la organización hacia una cultura de autocontrol, puesto que su seguimiento no solo puede ser generado como parte de la auditoría, sino también puede ser relevado a los dueños de proceso como primera línea de defensa y respuesta a la gestión de riesgos.

Factores claves de éxito para la implementación de data analytics

Cada organización tiene diferentes necesidades y visiones para D&A, a medida que las organizaciones buscan planificar su implementación deben considerar los componentes básicos de D&A descritos en la gráfica No.11.

En Colombia ya existen organizaciones multilatinas, que han tomado la decisión de trascender en sus funciones de auditoría, adoptando modelos avanzados e integrados con el uso de data analytics para su desempeño, teniendo a la auditoría interna como un aliado estratégico para el fortalecimiento del sistema de control interno, el mejoramiento de la cultura de gestión de riesgos y apoyo en el logro de los objetivos estratégicos, siendo éste el principal reto que podamos manejar desde nuestra perspectiva.

Gráfico 11. Componentes básicos de D&A



Fuente: KPMG - Presentación "Integrating data & analytics within internal audit"

1.5 El Pensamiento crítico y lo que se espera de los auditores

En una economía incierta y desafiante, las organizaciones están buscando un enfoque de auditoría interna que vaya más allá de revisar las actividades pasadas. Las organizaciones quieren auditorías internas que sean más ágiles, que adicionalmente se proyecten a anticipar hacia el futuro y que vayan más allá de preservar el valor para crearlo a nivel de la organización.

Para cumplir con estas expectativas, los líderes de auditoría interna deben enfocar sus esfuerzos a lograr una mayor madurez y así lograr que evolucionen los procesos y habilidades de auditoría básica a un enfoque para crear valor y conocimiento.

En ese orden de ideas, aplicar el pensamiento crítico a la auditoría interna es más que un simple ejercicio de planificación, es uno que permite la transformación de alguna manera a cada elemento del proceso de auditoría.

El pensamiento crítico puede expandir o desarrollar la percepción positiva de las áreas en toda la organización.

Veamos una descripción de lo que significa el pensamiento crítico en el contexto de la auditoría interna:

Pensamiento Crítico

El pensamiento crítico es un enfoque de mente abierta para analizar una situación o tarea para el desarrollo de conclusiones compatibles y transmitir los resultados evaluados de una manera lógica.

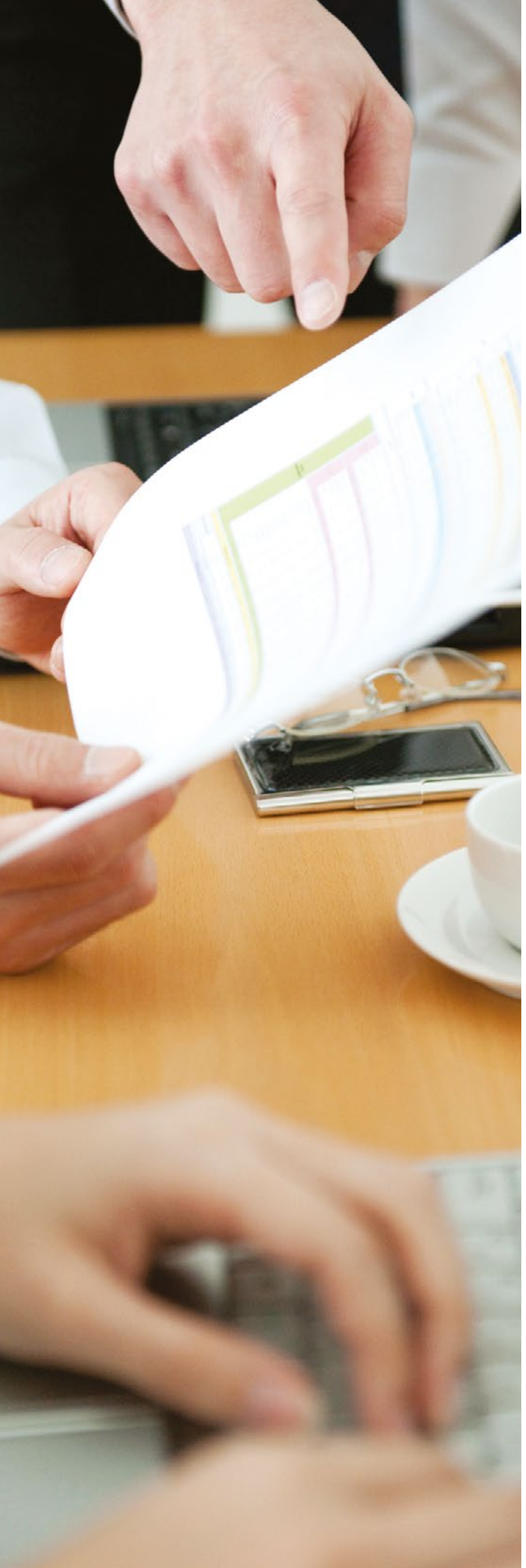
El pensamiento crítico incluye:

- Cada elemento del proceso de auditoría interna debe ser desafiado.
- Identificación de nuevas interdependencias de procesos, entradas, relaciones y oportunidades.
- Establecer la auditoría interna como socio estratégico centrado en lograr el equilibrio entre la gestión de riesgos y el rendimiento del negocio.
- Proporcionar valor tangible a una organización.

La siguiente pirámide de madurez (gráfica 12) de la función de la auditoría Interna detalla el rol que desempeña el pensamiento crítico:

Gráfica 12: Pirámide de madurez de la función de la auditoría interna

Fuente: Información tomada de KPMG



a) Habilidades de auditoría

La auditoría interna está estructurada para permitir el mantenimiento de la independencia y la objetividad, así como la proximidad al negocio. En el núcleo de cualquier auditoría se encuentran los rasgos fundamentales del auditor, que a su vez sirven como base para involucrar el pensamiento crítico en las auditorías:

- Escepticismo profesional: el impulso para profundizar en mostrar el instinto del auditor y hacer preguntas: qué, por qué, quién, cuándo y cómo. Las normas de auditoría definen el escepticismo profesional como una actitud que incluye una mente inquisitiva, estar alerta a las condiciones que pueden indicar falencias posibles debido a errores o fraude, y una evaluación crítica de la evidencia de auditoría.
- Comunicación: poder expresar de manera eficiente las ideas escritas y verbales a los interesados.
- Escuchar: comprender los objetivos del departamento auditado, los plazos y las barreras, aumentando así su confianza en la auditoría interna.
- Maneje lo inesperado: sea ingenioso, ágil y capaz de reaccionar rápidamente en formas creativas para desarrollar una solución.
- Preparación: garantizar un enfoque ingenioso para ser plenamente consciente y analizar la información disponible.

b) Conocimiento de procesos, organización y tecnología.

La auditoría interna debe estar estructurada para abordar riesgos clave y satisfacer las expectativas de los interesados. Esto significa una comprensión profunda de la organización y los negocios para aplicar el juicio y desafiar a la empresa en una amplia gama de temas.

Los puntos clave del conocimiento necesario incluyen:

- Procesos de negocios que contengan entradas importantes, resultados e indicadores clave de rendimiento,
- Conocimiento de la organización más allá de lo básico: personas influyentes clave, dinámicas culturales, iniciativas y proyectos estratégicos principales, eventos de cambio transformacional y percepción de auditoría interna,
- Claridad en los roles y responsabilidades, incluida la delegación de autoridad de sistemas o herramientas de aplicación clave: saber qué recursos de datos están disponibles para aprovechar.

c) Experiencia en la industria

La auditoría interna tiene una importante responsabilidad cada período para identificar las habilidades y competencias necesarias para entregar el plan anual de auditoría interna. La experiencia de la industria es una constante en este entorno cambiante y debe incluir:

- Conocimiento de la industria, tendencias de negocios y eventos actuales para permitir discusiones efectivas de los interesados.
- Anticipar las tendencias emergentes con el impacto organizacional y el impacto potencial de la auditoría interna.
- Aumentar y cambiar el panorama regulatorio y de cumplimiento dentro de la industria.
- Pulso del mercado competitivo.
- Reconocimiento de marca y posición de la empresa con los clientes.
- La auditoría interna debe evaluar críticamente y de forma integral cada una de las áreas e identificar fortalezas y debilidades.

Analizando la experiencia en la industria

- Un equipo de auditoría interna es tan bueno como el talento disponible.
- La auditoría interna en muchas organizaciones no se considera un destino profesional, sino un sistema "proveedor de valor" para las organizaciones o funciones en crecimiento.
- Como sistema proveedor, la auditoría interna puede enfrentar períodos de limitaciones de experiencia a medida que se reemplazan las transferencias fuera de las áreas o de la organización.
- Esto puede crear la necesidad de recurrir a profesionales especializados para proporcionar una perspectiva más amplia. Estos profesionales pueden provenir internamente de la organización o de consultores externos con las habilidades y experiencia necesarias.

d) Pensamiento crítico

En este nivel de madurez, la auditoría interna se caracteriza por una cultura de desafío, sondeo y mejora continua.

Los siguientes son elementos fundamentales en un enfoque de pensamiento crítico para la auditoría interna:

- Mentalidad abierta: reconocimiento de alternativas y evaluación de supuestos y consecuencias razonables.
- Análisis de la situación: capacidad para desglosar el problema en los componentes con respaldo fáctico para proporcionar una comprensión más profunda y claridad de los desafíos.
- Proporcionar contexto: identificación de lo que se conoce, lo que no y lo que los comparativos proporcionan contexto.
- Lluvia de ideas: canalizar ideas prácticas en un análisis más detallado o soluciones detalladas.
- Concluya: colóquelo todo de manera creativa en un formulario completo que proporcione la recomendación más adecuada.

e) Creación de valor

En este nivel de madurez, la auditoría interna es más que una función de cumplimiento centrada solo en preservar el valor. Las invitaciones se extienden para que la auditoría participe en reuniones clave y sirva como componente para la toma de decisiones. Por ejemplo:

- Cambio de sistema: actúe como asesor de la empresa para garantizar que los procesos o controles de información no se pierdan, sino que se mejoren cuando los sistemas hacen la transición.
- Mejora administrativa y operacional: se conserva como un enlace de riesgo para ayudar a asegurar que sean identificados y evaluados por la organización y los controles no se eliminen o se generen nuevos riesgos cuando se cambian los procesos.
- Iniciativas estratégicas: evaluaciones en tiempo real de nuevos productos, innovaciones y nuevos mercados.
- Las partes interesadas solicitan actividad de auditoría.

En conclusión mediante la inclusión de los anteriores aspectos de pensamiento crítico en todo el ciclo de una auditoría el resultado final será una auditoría más dinámica que no solo se enfoca en los riesgos y controles subyacentes, sino que también genera una mentalidad de valor para la organización a través del enlace de todas las interdependencias asociadas con el área bajo revisión.

Lo que se espera de los auditores

Basados en algunas premisas del ambiente empresarial en el que se desarrollan los auditores, como es, la aparición de entornos más sofisticados cada vez más con mayor fuerza, la adopción de nuevos marcos normativos alineados con el contexto internacional, la evolución de los negocios por los convenios gubernamentales con potencias económicas líderes en prácticas económicas y transaccionales de vanguardia, el uso de la tecnología en la automatización de la información y el mismo cambio generacional de los grupos de interés, entre otras, impulsa de forma exponencial a que el auditor se deba adaptar rápidamente en la misma dirección.

Las preguntas son ¿Estamos listos?, ¿comprendemos realmente todos los riesgos involucrados y los podemos atender con nuestras competencias?, ¿conocemos la perspectiva de la práctica líder en la industria?, ¿hemos utilizado información de análisis de datos de una variedad de fuentes para llegar a la causa raíz de los problemas y centrarnos en lo que realmente nos preocupa? es decir, ¿consideramos los datos estructurados disponibles de los sistemas y los datos no estructurados disponibles interna o externamente?, ¿cuál es el valor tangible que le estamos proporcionando al negocio en cada auditoría?

Por tales cuestionamientos, se prevé que el perfil del auditor, sin perder su esencia independiente de transmitir confianza, se enfocará en promover el desarrollo de nuevas competencias y habilidades técnicas, profundizar en el apoyo gerencial y la generación de valor agregado a la alta dirección y el gobierno corporativo como una disciplina aliada en la toma de decisiones al instante en las organizaciones.

Para lograr dichos propósitos, desde la academia y pasando por el espacio laboral se ha tenido que realizar un proceso de desaprender y volver a interiorizar los conceptos técnicos que encierran los nuevos enfoques de auditoría con un objetivo propio que persigue en primera instancia estabilizar en sus integrantes los conceptos y reglas técnicas que la rigen.

Nos espera consolidar nuevos desafíos del ejercicio de la auditoría en la creación de valor en la sociedad y en las organizaciones, como por ejemplo, el pensamiento crítico mencionado en el punto anterior, que trascienda más allá de los elementos básicos de una organización, la disrupción tecnológica por la entrada de la robótica aplicada en los diferentes procesos de las organizaciones, el análisis sistemático de los datos y no dejar de lado el cambio generacional.

Es importante considerar que nuevos conceptos como Big Data que se puede entender como grandes datos o altos volúmenes de datos con una configuración estructurada, semiestructurados o, sin estructurar que permiten tomar decisiones de negocio con una visión futurista, requieren del rol activo de auditores que confirmen la integridad de los datos, también, si consideramos en parte a la auditoría como esa exigencia que tienen todas las organizaciones de contar con un control estricto de sus procesos que se traduce en información para la correcta y oportuna toma de decisiones, sería un error pensar que no es necesario la exigencia de trascender en la aplicación de estándares tradicionales y de perfiles estáticos en la práctica de auditoría.

Por lo anterior, la necesidad de seleccionar ciertas habilidades en los procesos de reclutamiento de los auditores para la función de auditoría.

Algunas de las habilidades que beneficiarían a la auditoría Interna y que requieren desarrollar los futuros auditores incluye:

- IT - automatización del entorno de control interno.
- Certificaciones específicas según el contexto donde se desempeñe: Se puede considerar, entre otras, Six Sigma (Metodología de mejora de procesos), CFE (Certified Fraud Examiners), CFA (Chartered Financial Analyst), CIA (Certified Internal Auditor), CFSA (Certified Financial Services Auditor), CISA (Certified Information Systems Auditor).

2. Auditorías de valor

2.1 Transformando la función de auditoría interna

La forma en que los auditores desarrollan la función de auditoría interna no solo debe fundamentarse en el conocimiento técnico y operativo de una organización, sino también en el estratégico; generando planteamientos por parte de los Directores de Auditoría como:

- ¿Está el plan de auditoría interna (AI) alineado con las iniciativas y objetivos estratégicos definidos por la organización?
- ¿Qué necesitan y quieren los grupos de interés de la función de AI?
- ¿Está la función de AI alineada con esas necesidades y expectativas?
- ¿Es el posicionamiento de AI, personas y procesos adecuados para satisfacer las necesidades de los grupos de interés?

Estas y más preguntas surgen a diario cuando se lidera una función de auditoría. De acuerdo con una encuesta realizada por KPMG Internacional en marzo 2017 sobre el valor estratégico de la auditoría interna, 99% de los encuestados identificó que la Alta Dirección espera que las funciones de auditoría interna desarrollen una labor más estratégica, caso contrario ocurre con la percepción de los Directores de Auditoría Interna, que describen su función como un 60% dedicado a lo estratégico y un 40% dedicado a actividades de soporte.

A través de una visión futurista y de aplicación de mejores prácticas, el rol de la auditoría interna debe estar de lado de la estrategia de transformación y crecimiento de las organizaciones; es decir, debe tener conocimiento de cuáles son las principales tendencias macro comerciales (nuevos productos), si la administración está en desarrollo de un proyecto de expansión de los negocios e infraestructura, si está planeando hacer o ejecutando proyectos de inversión de capital, si se están dando cambios a nivel organizacional, si existen nuevas oportunidades estratégicas; ser consciente de la velocidad del cambio tecnológico, de señales de crecimiento económico, entre otras, que influyen en la transformación del negocio. La función de auditoría interna puede desempeñar un papel importante en el apoyo de programas y proyectos exitosos de la empresa.

Los beneficios de tener una auditoría interna en el proceso de transformación y crecimiento de la organización, son:

- Implementación de prácticas líderes que pueden llevar a múltiples beneficios corporativos y ventajas competitivas:
  - Procesos mejorados de gestión de riesgos.
  - Ambiente de control mejorado.
  - Fortalecimiento de las relaciones con los principales interesados.
  - Mayor eficiencia en las actividades clave de gobierno, riesgo y cumplimiento (GRC).
  - Identificación de mejoras en los procesos, reducciones de costos y mayor rentabilidad.
- Obtención de una auditoría interna certificada, bajo estándares globales.
- Optimización y apoyo en el refuerzo de los controles, reducción de los riesgos, identificación eficiencias potenciales y obtención beneficios de costos, de los elementos foco de transformación; dado que, todo cambio conlleva a riesgos complejos y emergentes.
- Identificación de las oportunidades significativas de crecimiento: mercados emergentes, productos potencialmente nuevos, proyectos como supervisor de aseguramiento de gobierno, riesgos y control.
- Continuo desarrollo y mejora del modelo operativo para un negocio en expansión, manteniendo marcos sólidos de estructura y desarrollo de la función de auditoría interna.

Con la transformación de la auditoría interna, ésta ha dejado de ser policiva y reactiva, es decir, de mostrarse cómo un equipo de inspectores que solo buscan errores o investigan situaciones ya ocurridas para denunciarlas en sus informes, a una auditoría asesora, que contribuye en el mejoramiento de los procesos, en la reducción de costos y apoyo en el cumplimiento de los objetivos estratégicos ; en la tabla 1 se detallan algunas características en la evolución de la auditoría.

Tabla No. 1. Evolución de la auditoría

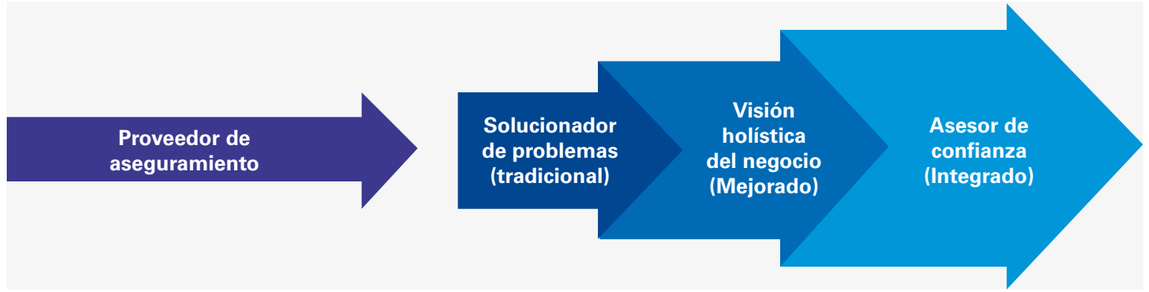
Auditoría Interna Tradicional	Auditoría Interna Consultiva
1. Vista solo como una función de cumplimiento.	1. Tiene un enfoque más colaborativo, aunque desafiante e intuitivo.
2. Realiza controles y auditorías financieras.	2. Está orientada en las áreas claves a fortalecer en la organización.
3. Identificación de auditorías a través de un enfoque cualitativo.	3. Ayuda a las áreas de negocio a administrar el riesgo y a que su desempeño sea más eficiente.
4. Coordinación limitada en la cobertura de riesgo.	4. Tiene una mayor comprensión y conciencia empresarial.
5. Centrada en la detección de problemas y errores.	5. Mayor implicación e integración en la estructura de gobierno.
6. La producción de auditoría es una prioridad.	6. Una función con mayor credibilidad por ser una auditoría interna certificada.
7. Enfocado en el cumplimiento de políticas y procedimientos.	7. Cuenta con un equipo de auditoría interna certificado en normas internacionales de auditoría.
8. Puede ser percibida como una actividad adversa	8. Ejerce sus actividades a través de las decisiones tomadas a nivel estratégico.
	9. Oportunidad en la identificación de brechas a través del monitoreo continuo de riesgos y controles.
	10. Ejecución de auditorías a través de análisis de datos (D&A) para tener un mayor cubrimiento en la información.

Fuente: Metodología de KPMG, en rol del auditor interno en la transformación organizacional.

> *De acuerdo con el nuevo enfoque de una auditoría de valor, ¿está seguro que el aseguramiento activo y continuo de los riesgos que trae un cambio organizacional, están siendo gestionados de manera efectiva?*

En el gráfico 13 se relaciona el rol en evolución de la función de auditoría interna.

Gráfico 13. Evolución de la función de auditoría interna



Fuente: Metodología de KPMG, en rol del auditor interno en la transformación organizacional

Las funciones de auditoría interna con los más altos estándares de desempeño se han ganado el papel de asesor confiable al brindarles a la organización, las personas y habilidades adecuadas para generar calidad y valor como resultado de las auditorías ejecutadas, no solo guiándose de los estándares internacionales de auditoría interna, sino también validándolas a través de un programa de mejora y aseguramiento de calidad (evaluación interna y externa) y la consecución de la certificación de la función, fomentando la credibilidad, el valor de la auditoría interna y promoviendo su rol dentro de la estructura de gobierno de la organización.

Respecto al programa de mejora y aseguramiento de calidad, el reto más grande al que puede aspirar una función de auditoría interna es obtener y mantener la certificación que soporta que sus actividades son realizadas de acuerdo con las Normas para el Ejercicio Profesional de la Auditoría Interna, el Código de Ética y las expectativas de la Alta Dirección y el Comité de Auditoría. Esta certificación da un respaldo internacional debido a que brinda las mejores prácticas para ejecutar la función de auditoría a nivel global, brinda credibilidad a los stakeholders y es un apoyo a las actividades que respaldan la profesión, promoviendo una comprensión más profunda del rol de la auditoría interna en el mecanismo de gobierno de las organizaciones.

Dentro de los elementos requeridos para asegurar la calidad de la función de auditoría interna, están:

- Las evaluaciones internas y externas de calidad.
- El monitoreo interno, es decir, evaluación y seguimiento de indicadores de gestión de la función – KPI´s (Ver tabla No. 2 - Ejemplo de los principales indicadores de desempeño de la función de auditoría interna - Cuadro de Mando de Auditoría Interna).
- La continuidad en la aplicación del programa de aseguramiento y mejora a la calidad.
- La evolución del nivel de madurez de la función de auditoría interna en el tiempo.
- El análisis de la percepción y la evaluación de la efectividad de la auditoría interna por parte del Comité de Auditoría, y
- El aseguramiento de que la actividad de auditoría interna está cumpliendo con las normas y el Código de Ética del IIA, a través de estos criterios de evaluación:

1

"Cumple Generalmente"

Esta es la máxima calificación, lo que significa que la auditoría interna tiene un estatuto, políticas y procesos y la ejecución y los resultados de éstos cumplen con las normas".

2

"Cumple Parcialmente"

Se considera que la práctica de auditoría interna tiene deficiencias que la apartan del cumplimiento de las Normas, pero éstas no impiden que la actividad de auditoría interna desempeñe sus responsabilidades".

3

"No Cumple"

Se considera que la práctica de auditoría interna tiene deficiencias que son tan significativas que impiden seriamente el desempeño adecuado de sus responsabilidades, en toda su actividad o en áreas relevantes".

Fuente: *KPMG a partir de las definiciones de la Norma 1320 del IIA, así: El director ejecutivo de auditoría debe comunicar los resultados del programa de garantía y mejora de la calidad a la alta dirección y al consejo.*

Finalmente, el propósito del programa de Evaluación de Calidad – Quality Assessment (QA), puede resumirse en tres conceptos clave:

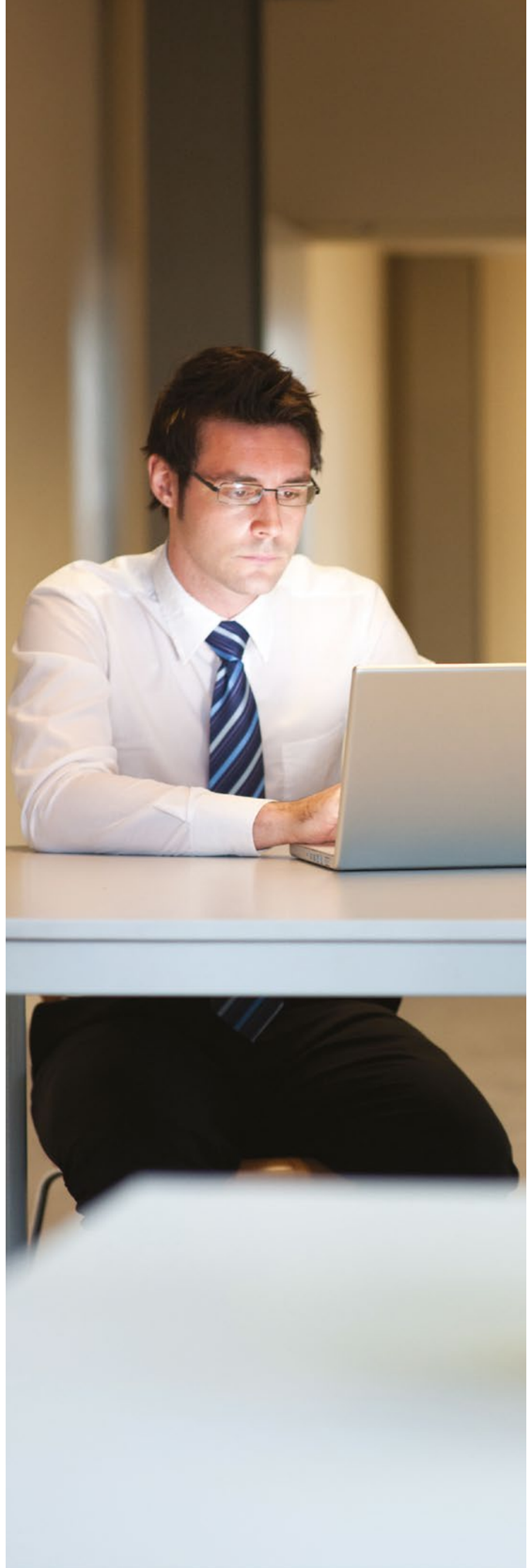
- Evaluar la eficacia de la actividad de auditoría interna al proporcionar servicios de aseguramiento y consultoría a la Dirección, el Comité de Auditoría, los altos ejecutivos y otras partes interesadas.
- Evaluar el cumplimiento de las normas y proporcionar una opinión sobre si la actividad de auditoría interna general cumple con ellas. Identificar oportunidades, ofrecer recomendaciones para el mejoramiento y proporcionar asesoría al responsable de la actividad de auditoría interna (Director Ejecutivo –DEA-, Auditor General, Gerente, entre otros) y al personal de AI para mejorar su desempeño y servicios, y promover la imagen y credibilidad de la función de auditoría interna.
- La auditoría interna se compromete con la mejora de las actividades que ejecuta, apoyando a la organización en el cumplimiento de los objetivos estratégicos.

Transformar la auditoría interna no sólo es una tarea del equipo que desempeña esta función, es un compromiso que se debe tener desde la Junta Directiva, el Comité de Auditoría y la Alta Dirección de una organización, para permitir la participación activa del Director de Auditoría Interna y su equipo en las actividades de la organización con la premisa clara de no perder la independencia que la debe caracterizar.

Tabla No. 2. Indicadores de gestión de la función de AI

Categoría	Propuesta de valor de la función de auditoría interna	Indicadores clave de desempeño
Personas	Direccionamiento y desarrollo de los recursos necesarios para ejecutar el plan anual de auditoría.	• % de las personas de la función con certificaciones profesionales o habilidades especiales (Ej. Auditores de TI). • % del plan de auditoría ejecutado por cada funcionario. • % del tiempo de reuniones destinado a entrenamientos y capacitaciones. • Promedio de los años de experiencia en funciones de auditoría. • Promedio del uso de recursos de acuerdo a su cargo. • Rotación por categoría.
Procesos	Optimizar la cobertura de los riesgos basándose en las inversiones y apetito de riesgo establecido por el Comité de Auditoría.	• Total de horas de ejecución frente a horas presupuestadas. • Uso de una metodología estándar y papeles de trabajo automatizados. • % de reportes emitidos en un lapso de trabajo de campo de xx días. • % de auditorías utilizando técnicas asistidas por computador y/o D&A. • Tendencias de los indicadores internos de aseguramiento de calidad. • # de quejas relacionadas con la función de auditoría interna.
Posicionamiento	Comprensión de la función de auditoría interna como un recurso estratégico para la organización.	• Cumplimiento del plan de auditoría con base en los 10 riesgos estratégicos de la compañía. • # de proyectos de auditoría relacionados con los objetivos estratégicos. • % de los recursos provenientes del programa de desarrollo empresarial. • # de sesiones de actualización a los miembros del Comité de Auditoría en el año. • # de proyectos especiales requeridos por la Alta Gerencia. • Resultados del Comité de Auditoría y riesgos y encuestas de satisfacción a la Gerencia.
Valor agregado y recuperación económica	Maximizar el valor financiero mediante la mejora continua de: • La gestión de riesgos y controles asociados a los procesos clave de la organización. • Eficiencia y efectividad operacional de los procesos y áreas clave de la organización.	• % de los hallazgos de auditoría considerados por la gerencia como significativos. • % de los planes de acción implementados en el año (últimos 12 meses). • # de oportunidades de mejora de los procesos. • Cantidad de ahorro/rentabilidad o valor recuperado como porcentaje de la implementación de los hallazgos de auditoría interna: – Aumento de la eficiencia y efectividad de los procesos (Ejemplo: tiempo de ciclo, resultados) – Reducción en costos de los procesos. – Reducción en los costos de controles en procesos o a nivel de entidad (SOX)

Fuente: KPMG , ejemplo de cuadro de mando de la función de auditoría, de acuerdo con la metodología de KPMG para evaluaciones externas de calidad.



2.2 La cultura de riesgo organizacional

Independiente del tipo de organización, la principal preocupación de la Alta Dirección está en enfocarse en los principales riesgos financieros que puedan afectar el cumplimiento de los objetivos estratégicos (riesgo de mercado, liquidez, crédito, entre otros), sin embargo, se debe tener una visión integral del negocio, donde es importante considerar otros aspectos que pueden afectar los resultados, como pueden ser deficiencias en la cultura organizacional, faltas a la ética de los empleados, incumplimientos legales o regulatorios, carencia de tecnologías que soporten los procesos, falta de investigación e innovación en los procesos, debilidades en seguridad informática y en seguridad ambiental, entre otras. Ver Gráfico 14.

Gráfica 14. Descripción de la gestión integral de riesgos

Fuente: KPMG construcción propia.

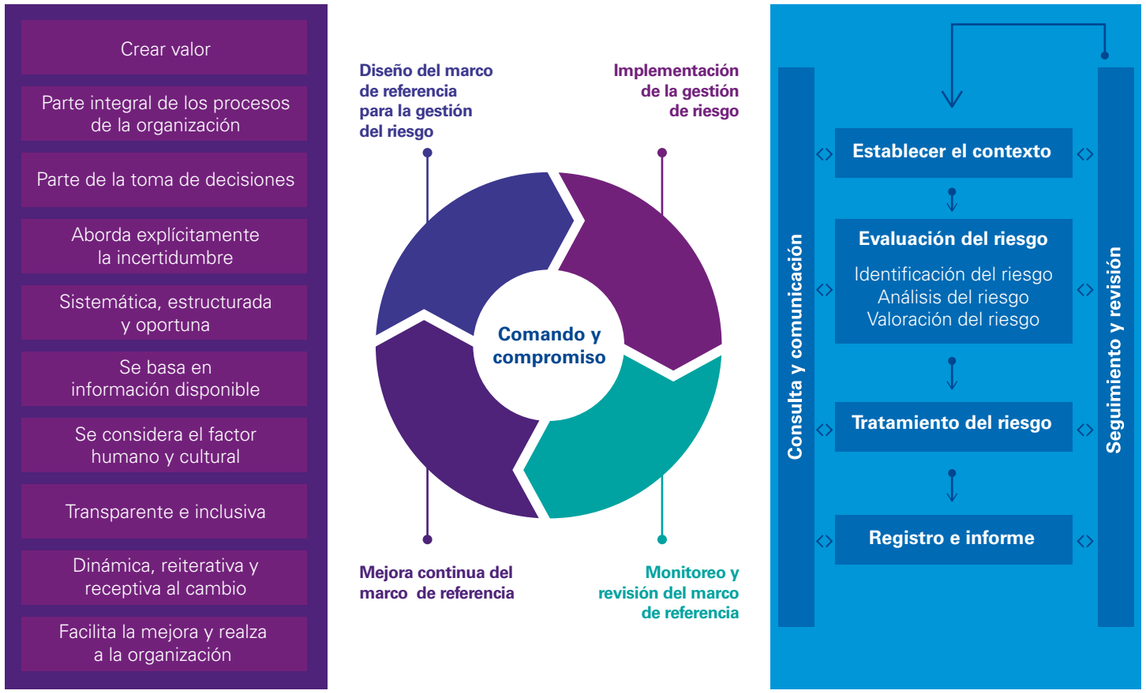
Estas situaciones se presentan por el dinamismo y la alta competitividad de los mercados, el desconocimiento de los procesos y su interacción con el resto de actividades de una organización, exponiendo diariamente al negocio a una serie de riesgos sin identificación o sin una adecuada gestión para mitigarlos, evitarlos o minimizarlos.

Dentro de la cultura de la gestión del riesgo organizacional, es relevante generar conciencia en el talento humano, como uno de los factores más sensibles por la importancia de las actividades que desempeñan los funcionarios desde cada uno de sus roles; ya sea directivo, profesional, técnico, operativo o asistencial, con una visión holística de sus procesos, teniendo en cuenta otros aspectos como la tecnología que soporta estas actividades, la regulación normativa aplicable a cada uno y las posibles afectaciones e impactos al medio ambiente.

De acuerdo con una publicación realizada por KPMG en Colombia en el 2017 denominada "La gestión de riesgos es lo que más preocupa a los Comités de Auditoría" se cita que "…Según los resultados, los comités de auditoría en general tienen confianza en la información financiera y en la calidad de la auditoría. Para los encuestados, los principales desafíos a los que se enfrentan las organizaciones son el comportamiento ético, cumplimiento legal/regulatorio, el riesgo de seguridad informática, los controles de la organización en torno al riesgo y la autoridad en la cultura organizacional…", la gestión de riesgos, que no es otra cosa que el manejo estructurado de la incertidumbre que puede generar una amenaza, mediante una serie de actividades que permiten la identificación, análisis, evaluación, tratamiento, comunicación y monitoreo regular de riesgos, se ha convertido en parte vital de las organizaciones.

La gestión de riesgos se basa en los principios, el marco de referencia y en los procesos que hagan parte de las organizaciones, con el fin de gestionar cualquier tipo de riesgo de manera eficiente, eficaz y coherente. Gráfica 15.

Gráfica 15. Principios, marco de referencia y procesos.



Fuente: Norma Técnica Colombiana NTC-ISO 31000 Gestión del Riesgo - Directrices del 18 de julio de 2018.

Este auge de gestión de riesgos, es una gran oportunidad para las área de monitoreo y control, ya que la información generada por los ejercicios de auditoría generalmente son de valor y conllevan oportunidades valiosas para mejorar los negocios en las diferentes organizaciones, impulsando la importancia de gestionar todos los riesgos que las pueden afectar (no solamente los riesgos financieros), mediante una adecuada administración de los mismos.

Para lograr este objetivo, es muy importante que los auditores internos en las organizaciones consideren como mínimo:

- Disponer de un grupo responsable encargado de liderar la gestión de los riesgos (diseño, implementación, supervisión y monitoreo).
- Implementar un proceso claro de evaluación de riesgos, en donde se involucren a las gerencias en la identificación y medición de los mismos, mediante la interacción con personal clave que participen de manera periódica en estas actividades.
- Determinar el tipo de información de riesgos a reportar que puedan afectar el cumplimiento del objeto de negocio de las organizaciones. Identificando claramente los riesgos claves del negocio, los cuales deberán ser reportados de manera periódica a las altas directivas considerando la probabilidad de ocurrencia, su impacto, los controles implementados para su mitigación y los mecanismos de monitoreo definidos para cada uno de ellos.
- Disponer de mecanismos que permitan determinar la adecuada supervisión de los riesgos, como por ejemplo los Comités de Auditoría, quienes serán los encargados de la supervisión de los principales riesgos de las organizaciones.
- Asignar responsables para cada uno de los riesgos, quienes serán los encargados de definir claramente los factores generadores de riesgos y los mecanismos implementados de control para minimizar o evitar que estos se presenten.

Lo anterior, permite a las auditorías presentar a la alta dirección:

- Resultados sobre la revisión efectuada a los riesgos claves.
- Evaluar los procesos de administración y gestión de riesgos.
- Dar concepto sobre los informes generados por las organizaciones sobre la administración de riesgos claves.

2.3 Gestión integral del riesgo en salud

Luciano Anneo Senneca un filósofo romano decía que "Cuando se está en medio de las adversidades, ya es tarde para ser cauto". Esta frase que parece sacada del sentido común, se aplica muy bien al tema actual de la salud en Colombia, ya que a pesar de que los actores sanitarios hablan de prevención en salud desde hace décadas, esta prevención no ha hecho introspección en la dirección del sistema y prueba de ello es un modelo de atención altamente asistencialista.

Es por ello que en un esfuerzo del gobierno por cambiar este panorama se establece a través de la resolución 429 de 2016 la Política de Atención Integral en Salud (PAIS) y el Modelo de Atención Integral en Salud (MIAS), colocando el enfoque de riesgos como un eje central y direccionando a las Entidades Administradoras de Planes de Beneficios de Salud (EAPB) e Instituciones Prestadoras de Servicios (IPS), a no solo gestionar los riesgos de su población, sino además a reconocer, evaluar y mitigar sus propios riesgos institucionales para lograr el mejor nivel de salud, una mejor experiencia de los usuarios y costos acorde con los resultados (MSPS; 2016).

El presente capítulo, está dividido en dos partes; en la primera, se introducirá al lector al tema con el enfoque de determinantes en salud y cómo estos complementan la Gestión Integral de Riesgos en Salud (GIRS). En la segunda parte, se abordarán los riesgos a los que están expuestos todas las instituciones de salud, para después terminar sugiriendo la aplicación de la metodología Enterprise Risk Management (ERM), como una herramienta que puede ayudar a las organizaciones de salud a mejorar su gestión de riesgos organizacional.

1. Gestión integral del riesgo en salud (GIRS)

Es un mecanismo que permite anticiparse a los eventos o materialización de los riesgos en salud y posibilita la respuesta o tratamiento oportuno para mitigar la evolución y/o complicación de los riesgos y sus consecuencias. La GIRS debe ser permanentemente monitoreada por la función de auditoría interna especializada en salud, en especial para los procesos clínicos, así como también se debe observar el cumplimiento de la normatividad aplicable a las entidades que tienen a cargo el aseguramiento y la atención integral en salud de los riesgos de salud de una población.

Esta gestión individual o colectiva, inicia con la identificación y el entendimiento de los factores determinantes del proceso salud-enfermedad, teniendo en cuenta que existe un amplio rango de determinantes de la salud, tales como las condiciones de vida y laborales, factores genéticos, socioeconómicos, ambientales y culturales que interactúan para determinar la situación de salud de las personas los cuales se explicarán en la próxima sección. Estas etapas deben ser consideradas por la auditoría interna en el monitoreo y ejecución de su plan de auditoría.

En la gestión del riesgo es necesario analizar el histórico evolutivo del riesgo en salud individual y los factores determinantes asociados a la enfermedad y discapacidad, para posteriormente realizar acciones que disminuyan la exposición a la enfermedad y el manejo integral de la misma una vez se haya contraído; adicionalmente, minimizar los riesgos derivados de la gestión clínica de la enfermedad y su evolución.

Alternamente, se debe realizar una serie de intervenciones colectivas y preventivas aplicadas efectivamente a grupos de la población que impactan los principales determinantes de la salud y disminuir así, la probabilidad de ocurrencia de morbi-mortalidad, y la materialización de eventos relacionados por deficiencias en la prestación de los servicios de salud.

Para llevar a cabo todo lo anterior, es indispensable la articulación de diferentes entidades de salud en cabeza del MSPS y una adecuada caracterización y segmentación de la población, que permitan diseñar acciones de promoción y prevención, y la puesta en marcha de planes y acciones integrales de intervención colectiva, para obtener una respuesta más efectiva a los riesgos y en consecuencia su directa mitigación de los impactos en la salud pública.

Determinantes en salud

Cada población tiene características particulares que hacen poco efectiva una aplicación uniforme de los programas en salud; lo anterior es importante para tener herramientas que aborden e involucren a todas las comunidades. La gestión del riesgo dado que está avocada a prevenir y mitigar riesgos de las poblaciones con mayor razón no debe excluir esta premisa, por eso una manera de dar este abordaje integral es desde el enfoque de determinantes en salud impulsado por la Organización Mundial de Salud (OMS).

Estos determinantes en salud en la función de auditoría en términos generales, se podría considerar como las causas y/o detonantes de la mayor probabilidad e impacto en la materialización de los riesgos en salud, que igual deben ser identificados, prevenidos, tratados y reasegurados.

Los determinantes de la salud se describen como el conjunto de factores sociales, personales, económicos, de asistencia en salud y ambientales que pueden influir en la salud de un individuo o población y generalmente se pueden enmarcar en dos grupos: a) de responsabilidad multisectorial del estado, como son los determinantes económicos, sociales y políticos; y b) de responsabilidad del sector salud. Estos aunque también están dentro del accionar del estado, se dirigen específicamente al escenario sanitario mediante la articulación de las entidades gubernamentales responsables de la salud de la población en lo que se refiere a vigilancia y control, prevención y promoción, etc. (Villar, 2011).

El impactar los determinantes sociales de la salud (susceptibles de ser intervenidos), como se ha evidenciado anteriormente, es fundamental para mitigar la carga de enfermedad, dado que es la posibilidad de romper círculos a través de la prevención. En este sentido el estado como formulador y ejecutor de las políticas públicas debe ejercer un control efectivo de estos factores fortaleciendo así políticas tras e intersectoriales que mejoren las condiciones de las comunidades.

Grupos para la gestión integral del riesgo en salud

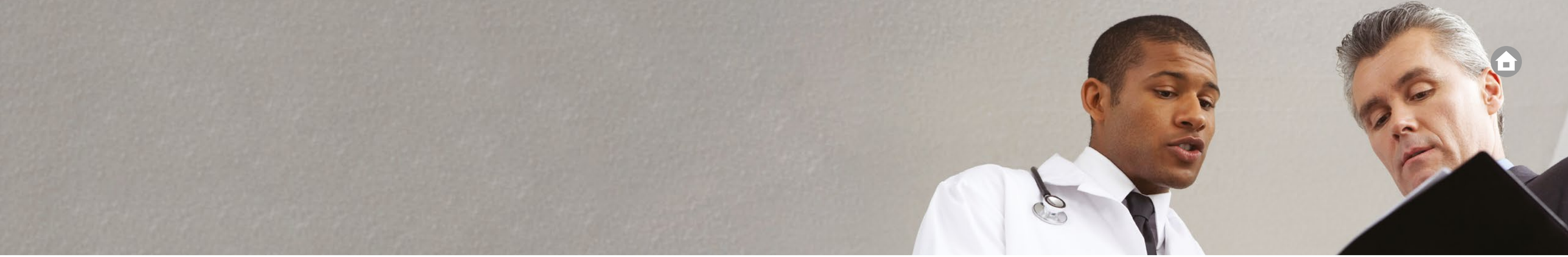
Para realizar una adecuada gestión del riesgo, es importante la identificación de grupos con características similares, bien sea económicas, demográficas o sociales, con una mayor exposición a los factores de riesgos que afectan su bienestar y desarrollo.

Estos grupos denominados Grupos de Riesgo, constituyen la base para la gestión integral del riesgo en salud y son definidos por el MSPS. Corresponden a los grupos poblacionales priorizados según un conjunto de eventos de interés en salud pública que comparten: i) la historia natural de la enfermedad y mecanismos fisiopatológicos causales, ii) factores de riesgo etiológicos, y relacionados, iii) desenlaces clínicos similares y iv) formas o estrategias eficientes de entrega de servicios.

Al poseer características similares, es posible definir una respuesta social organizada y coherente establecida como proceso de atención integral sectorial e intersectorial que permite su gestión integral. Es aconsejable para la función de auditoría interna elabore su plan de auditoría alineada a estos grupos.

Gráfica 16. Grupo para la gestión integral del riesgo en salud

Fuente: Adaptado del Ministerio de salud y protección social



Gestión integral del riesgo con rutas integrales de atención en salud (RIAS)

El MSPS define la atención integral de salud, como "el conjunto de acciones coordinadas, complementarias y efectivas para garantizar el derecho a la salud, expresadas en políticas, planes, programas, proyectos, estrategias y servicios que se materializan en atenciones dirigidas a las personas, familias y comunidades para la promoción de la salud, prevención de la enfermedad, diagnóstico, tratamiento, rehabilitación y cuidados paliativos" (MSPS, 2016).

Las RIAS, son un instrumento que involucra esa toma de decisiones y la organización del proceso de atención para los diferentes grupos de riesgo. También incluyen el conjunto de acciones poblacionales, colectivas e individuales a ser efectuadas, los destinatarios, los entornos donde se realizan y el tipo de institución responsable por su ejecución, así como las principales decisiones de seguimiento, y contribuyen a la estandarización y operatividad del modelo de atención previsto, la estimación de las necesidades de oferta de servicios y de recursos, al fortalecimiento de las relaciones entre prestadores y aseguradoras, y a evaluar el desempeño y resultados de la atención por los diversos agentes del sistema.

Lo anterior, a efectos de garantizar no solo el ejercicio del derecho sino a lograr la legitimidad del sistema de salud por parte del ciudadano, en una apuesta de Estado para el desarrollo de redes sociales de respuesta, la participación ciudadana activa y constructiva para la promoción de la salud y no solo de control social (MSPS, 2014).

2. Principales riesgos de las entidades de salud

La gestión de riesgos no solo puede ser aplicada a la población en general, sino que además puede realizarse a través de la identificación e intervención de los riesgos organizacionales que como organización tienen las instituciones sanitarias como las EAPB e IPS. Esto redundará entre otras cosas en mejorar la estabilidad estructural del sistema general de seguridad social y ayudará a predecir el comportamiento de dichas instituciones dado que están inmersas en una competencia regulada que sigue principios de mercado.

Las funciones de auditoría interna especializada en salud deben tener en cuenta y conocer en la planeación y desarrollo de su trabajo los principales riesgos en salud a los que está expuesta la población objetivo.

El primer paso en este sentido es la identificación de riesgos organizacionales los cuales pueden dividirse en seis grupos y que se deben tener en cuenta en la planeación:

- Estratégico: probabilidad de pérdida como consecuencia de la imposibilidad de implementar apropiadamente los planes de negocio, las estrategias, decisiones de mercado, la asignación de recursos, y la incapacidad de adaptarse a los cambios en el entorno de los negocios.
- Externo: su origen se localiza fuera de los sistemas especializados, pueden señalar descoordinación, intervención gubernamental, factores climatológicos y falta de planificación.
- Financiero: probabilidad de que una entidad no tenga la capacidad financiera para cumplir sus obligaciones de pago tanto a corto como a largo plazo. La situación de salud de los afiliados, la dinámica de la demanda de servicios, los cambios en la tecnología y la incidencia de eventos de alto costo, entre otros, influyen en el riesgo financiero de las entidades, quienes deben realizar acciones para contrarrestar su efecto.
- Operacional: probabilidad de que una entidad presente desviaciones en los objetivos de sus procesos como consecuencia de deficiencias, inadecuaciones o fallas.
- Gente: probabilidad de cambios permanentes en las condiciones de salud, cambios tecnológicos y escasez de recursos.
- Salud: probabilidad de ocurrencia de un evento no deseado, evitable y negativo para la salud del individuo, que puede ser también el empeoramiento de una condición previa o la necesidad de requerir más consumo de bienes y servicios, que hubiera podido evitarse (Plan Decenal de Salud Pública, PDSP, 2012-2021). El evento es la ocurrencia de la enfermedad o su evolución desfavorable y sus causas son los diferentes factores asociados (Resolución 1841 de 2013, pág. 51). El riesgo en salud a su vez puede clasificarse como primario si se refiere a la probabilidad de aparición de nueva morbilidad (incidencia), o como técnico si alude a la probabilidad de "ocurrencia de eventos derivados de fallas de atención en los servicios de salud y de la mayor carga de enfermedad por mortalidad evitable y discapacidad" (Resolución 1841 de 2013).

Como es de esperarse, este riesgo es el más relevante en las entidades del sector, dado que en el aseguramiento en salud, el riesgo visto desde la perspectiva epidemiológica se relaciona estrechamente con el riesgo empresarial, entendido como la probabilidad de generación de pérdidas económicas por la ocurrencia de un evento adverso derivado de las actividades propias del negocio (Resolución 1740 de 2008).

Este abordaje similar permite entonces, equiparar herramientas utilizadas a nivel empresarial y adaptarlas al sector salud con la acotación que existe una subdivisión clara entre los EAPB y las IPS (Jiménez, P., & Nereida, D., 2011).

La práctica de KPMG Healthcare, sugiere la metodología "ERM" Enterprise Risk Management para la gestión de riesgos empresariales ya que en particular para Colombia, dicha metodología se alinea con los requerimientos del modelo de Supervisión Basada en Riesgos "SBR" de la Superintendencia Nacional de Salud.

Sistema de gestión de riesgos para entidades del sector salud - Enterprise Risk Management "ERM" / ("SAR") Sistema de administración de riesgos

Los sistemas de administración de riesgos permiten hacer una efectiva gestión de los riesgos inherentes a la actividad económica de la empresa y evita la afectación de la viabilidad de su objeto mediante la identificación, medición, control y monitoreo de los posibles riesgos (Fasecolda, 2018).

Enterprise Risk Management (ERM) o Gestión de Riesgos Empresariales es una metodología que integra la gestión de riesgos con las oportunidades de alcanzar nuevos objetivos de negocio (Zenklussen, 2016).

Los principales aspectos que se deben tener en cuenta para la implementación de un ERM en entidades del sector salud son los conductores de su implementación: el gobierno corporativo, la estrategia y el desempeño. Más específicamente que la Junta Directiva se involucre profundamente en la definición y ejecución de la estrategia, que la estrategia se alinee con la calidad de la salud de los pacientes y el mejoramiento de la calidad de vida de la población, un excelente acceso a la información del riesgo con ciberseguridad, y por último, una comunicación efectiva entre la Junta Directiva y la alta dirección en la supervisión de los riesgos estratégicos y operacionales.

2.4 Auditoría interna en el sector de pensiones

Aspectos del sistema general de pensiones y su entorno social

El Gobierno Nacional creó el Sistema General de la Seguridad Social Integral en Colombia mediante la Ley 100 de 1993 y la Ley 797 de 2003 que reformó algunas disposiciones de la Ley 100. Con estas normas el Gobierno tiene el marco para el Sistema General de Pensiones con el fin de garantizar que la población colombiana tenga el cubrimiento contra las contingencias derivadas de la vejez, la invalidez y la muerte. Igualmente, dichas normas buscan ampliar la cobertura a grupos de la población colombiana que todavía no se encuentran en este sistema.

El Sistema General de Pensiones se encuentra conformado por dos regímenes solidarios cuyas características se explican en la tabla No. 3, los cuales no pueden estar mezclados pero pueden interactuar entre sí; por tanto, ninguna persona podrá estar en los dos regímenes de forma simultánea.

Tabla No.3 Características de los regímenes pensionales vigentes en Colombia.

Características de los Regímenes	
Régimen Solidario de Prima Media con Prestación Definida (RPM) "Administrado por Colpensiones"	**Régimen de Ahorro Individual con Solidaridad (RAIS) "Administrado por Fondos Privados"**
El otorgamiento de la pensión de vejez, invalidez, sobrevivencia o la indemnización sustitutiva dependen del cumplimiento de requisitos de ley. La pensión de vejez depende de las semanas cotizadas (mínimo 1.300) y de su ingreso base de liquidación (IBL). Requisito de edad es 62 años si es hombre o 57 años si es mujer. Si no hay derecho a pensión se da una indemnización sustitutiva. Los aportes constituyen un fondo común de naturaleza pública. El monto de pensión está previamente definido por la ley y es el estado quien garantiza el pago de los beneficios.	La pensión de vejez depende del capital que el afiliado tenga en la cuenta de ahorro individual y sus respectivos rendimientos financieros, al momento de pensionarse. Podría tener una pensión anticipada según su capital. Si no hay derecho a pensión se da una devolución de saldos. La pensión se causa cuando el capital acumulado permita obtener una pensión mensual superior al 110% del SMMLV, o cuando acceda a la garantía de pensión mínima.

Fuente: KPMG - Construcción propia a partir de la normatividad vigente.

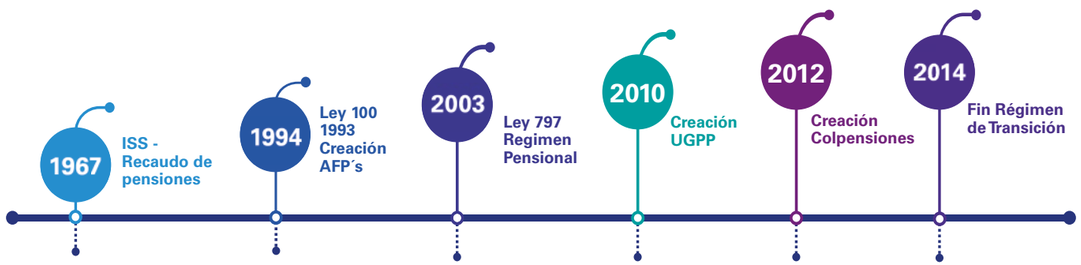
El Gobierno Nacional creó, de otra parte, la Unidad Administrativa Especial de Gestión Pensional y Contribuciones Parafiscales de la Protección Social - UGPP, con el fin de administrar los derechos pensionales ya causados y/o reconocidos del regimen de prima media público del orden nacional. Al 2018 esta entidad agrupa alrededor de 33 entidades públicas, con una nómina aproximada de 317.360 pensionados.

De los 49,8 millones de colombianos según Censo DANE-2018, solamente 19,8 millones (44%) están afiliados al sistema pensional; sin embargo, tan solo 7,7 millones (17%) están cotizando, lo que significa que solo uno de cada tres colombianos van a lograr pensionarse; frente a este escenario millones de colombianos tienen como una única opción aplicar a los beneficios que otorga el Gobierno como son los Beneficios Económicos Periódicos (BEPS) que ofrece Colpensiones, en el cual se hace un pequeño ahorro que al final de su vida productiva le garantizará al vinculado un valor mínimo y hasta un 80% de un SMMLV, y en el caso del Régimen de Ahorro Individual con Solidaridad (RAIS) una Garantía de Pensión Mínima, donde el Gobierno subsidia una parte del saldo que le haría falta para pensionarse, con el fin de obtener una mesada correspondiente al salario mínimo de la época o en su defecto una pensión familiar, que se reconoce por la suma de esfuerzos de cotización o aportes de cada uno de los cónyuges o compañeros permanentes cumpliendo en conjunto los requisitos establecidos para adquirir la pensión.

Una sombra en el Sistema General de Pensiones

En Colombia, están claramente definidos los regímenes vigentes y la normatividad establece los requisitos para la obtención de los derechos; sin embargo, la falta de control en los procesos, sistemas de información vulnerables, falta de ética en los funcionarios y sistemas judiciales corruptos, ha generado que se presenten defraudaciones al sistema pensional del país por el reconocimiento de pensiones a personas sin derecho o por montos superiores a lo permitido. Hoy las pensiones del RPM (Régimen de Primera Media) dependen casi completamente del presupuesto nacional y estos eventos han impactado de manera negativa el sistema pensional, afectando la confianza de la población cotizante, la imagen de las administradoras y el rompimiento del sistema

Gráfica 17. Eventos materializados de riesgos en el sector pensiones



Situaciones de crisis en el Instituto del Seguro Social – ISS

- Alteración en las fechas de nacimiento.
- Vinculaciones laborales falsas.
- Manipulación de semanas cotizadas.
- Pago efectivo de pensiones sin tener derecho.
- Exámenes y conceptos de las juntas de calificación de invalidez favorables para asignación de beneficios.
- Condena de pensionados, tramitadores, jueces y abogados.

Sistema afectado por estructuras criminales

Las causas identificadas que han dado lugar a estos eventos, están asociadas, según comunicado de prensa de la Fiscalía General de la Nación (abril 2019), con:

- Desconocimiento por parte de los beneficiarios o pensionados de la normatividad pensional.
- Documentos falsos para acceder a todo tipo de pensiones, en especial, de vejez y sobrevivencia.
- Presentación de certificados falsos para obtener beneficios.
- Manipulación de información.
- Tramitadores y abogados dedicados a engañar pensionados y al Estado.
- Jueces que abusan de su poder para dar órdenes/fallos ambiguos frente a la normatividad y facilitar el otorgamiento de beneficio de los recursos pensionales.
- Personas que se corrompen a fin de acceder a beneficios para los cuales no se ha ganado el derecho.
- Funcionarios y trabajadores que delinquen desde sus cargos.

Fuente: KPMG - Construcción propia a partir de información histórica y Fiscalía General de la Nación (abril, 2019)

respecto a sus objetivos primordiales que quiere el Estado para los colombianos, unido a una reforma pensional que según los expertos será necesaria para proteger efectivamente la vejez.

En la gráfica 17, se muestran algunos hechos de corrupción que se han presentado tanto en el liquidado Instituto del Seguro Social-ISS, como hoy en Colpensiones para el caso de Régimen de Prima Media y que han impactado de manera negativa el sistema.

De acuerdo con el informe de la Fiscalía General de la Nación, por pagos indebidos de pensiones se tiene conocimiento de aproximadamente 1.300 situaciones de presuntos fraudes, situación que alerta al sistema; las entidades administradoras y el Estado en general, han hecho amplios esfuerzos en la identificación de los riesgos relacionados con este sector, en realizar las investigaciones pertinentes por denuncias o indicios de malos manejos operacionales y han establecido controles que les permita minimizar los riesgos presentados, apoyándose en actores de control que puedan reforzar los escudos de protección en contra de estas acciones, que pueden conllevar a grandes desfalcos monetarios para el Estado.

La auditoría como herramienta de apoyo al control

Las organizaciones con un apoyo serio y coherente de la administración, la Junta Directiva y del Comité de Auditoría, deben propender por un sistema de control interno efectivo que brinde seguridad en el cumplimiento de políticas, procesos, procedimientos y comportamientos, a fin de propiciar un funcionamiento efectivo y eficiente, que contribuya al aseguramiento de la calidad e integridad de la información y ayude a garantizar el cumplimiento de la legislación aplicable.

En la actualidad las organizaciones ven a las auditorías como herramientas de apoyo estratégico y control para lograr el cumplimiento de los objetivos planteados, donde el papel fundamental es generar resultados de valor y encaminar a las organizaciones hacia el mejoramiento continuo. Así las cosas, las Administradoras de Pensiones y el Estado han visto la necesidad de involucrar a la auditoría en diferentes niveles de sus procesos, con el fin de lograr una administración eficaz y eficiente de sus recursos y operaciones, buscando minimizar los riesgos que tienen asociados al sistema general de pensiones, y más cuando existen

diferentes grupos de interés involucrados en el proceso que tienen sus propias expectativas frente al sistema.

La auditoría como apoyo a la gestión y prevención de los riesgos en las organizaciones ayuda a identificar, evaluar, y definir la exposición a los mismos, basados en esas necesidades, ha sido reconocida como parte esencial de las prácticas de un buen gobierno corporativo. Hoy en día, las organizaciones adquieren un enfoque donde la idea es identificar los riesgos asociados a su negocio y explicar cómo gestionarlos, y es precisamente la auditoría la que debe agregar valor a sus clientes a través de la revisión que permita asegurar que los riesgos están siendo monitoreados y administrados.

Aspectos relevantes en el sector de pensiones

El sector pensional se enfrenta a grandes retos asociados con robustecer procesos para asegurar el funcionamiento adecuado del sistema, implementar la robótica como apoyo a la operación, administrar la información de manera efectiva y eficiente (oportunidad y calidad), desarrollar e instalar sistemas de información seguros y debidamente controlados, gestionar los riesgos existentes, y anticiparse a lo que pueda impactar el logro de sus objetivos estratégicos; con base en lo anterior, la auditoría debe desarrollar una función de apoyo y asesoría a las organizaciones, identificando situaciones de riesgo que puedan afectar la operatividad, credibilidad, imagen, finanzas y continuidad de dichas entidades; la auditoría puede considerar los siguientes aspectos relevantes:

- Administración de riesgos inadecuado por políticas insuficientes, identificación, análisis y valoraciones incompletas o erradas.
- Identificación inadecuada o inexistencia de alertas de la operación que permitan identificar riesgos nuevos o emergentes.
- Asignación de accesos a los sistemas de información sin garantizar una adecuada segregación de funciones.
- Generación de conceptos jurídicos desalineados a la normatividad aplicable.
- Favorecimiento de procesos y otorgamiento de beneficios en contra de la organización.
- Contratación de personal sin el cumplimiento de los requisitos requeridos.
- Uso indebido de la información de la organización a través de los sistemas de información, o un alto componente de manualidad para la operación.
- Inoportunidad en el registro y respuesta a solicitudes de prestaciones económicas.
- Determinación de derechos prestacionales de forma errada y/o sin el cumplimiento de los requisitos, normas, directrices y lineamientos establecidos por la entidad.
- Liquidación indebida de la nómina de pensionados, por información errónea o fraudulenta.
- Pérdida de integridad de la información administrada por la organización.
- Incumplimiento de las políticas y lineamientos de inversión.
- Apropiación, desviación, o aplicación indebida de dineros, o recuperación inadecuada de valores adeudados a la organización.
- Procesos de contratación de proveedores que no cumplen con los requisitos normativos establecidos y de idoneidad.
- Traslado masivo de los fondos privados al régimen de prima media por fallos judiciales que favorecen a los afiliados.

Otro tema que preocupa igualmente al sistema es la información que se debe tener en cuenta para la determinación de las prestaciones económicas a las que un ciudadano podría tener derecho, es así como el Gobierno Nacional por medio del Decreto 726 de 2018[8] del Ministerio del Trabajo crea el Sistema de Certificación Electrónica de Tiempos Laborados (CETIL) como mecanismo para la emisión de certificaciones de tiempos laborados y salarios devengados por parte de entidades públicas y privadas, con el fin de ser aportadas a las entidades que reconozcan prestaciones pensionales a través del diligenciamiento de un formulario único electrónico, y así tener información en línea y certificada evitando la manipulación o fraude en la emisión de las misma por parte de terceros. Por tanto, ahora esto se vuelve también una preocupación en el sentido que esta información debe ser de alguna manera verificada con el fin de corroborar las fuentes utilizadas para certificar. Es importante señalar que la responsabilidad de la veracidad de la información certificada para establecer las prestaciones económicas es de quien la certifica, según el Decreto 1748 del 12 de octubre de 1995, para el caso de bonos pensionales; sin embargo, la Nación en cabeza del Ministerio de Hacienda tiene la potestad de realizar las comprobaciones que considere pertinentes.

Trascendencia de la auditoría - Un dato más o el poder total sobre la información

Hoy la tecnología ofrece herramientas[9] para el análisis de la totalidad de la información registrada en las bases de datos, que frente a las expectativas de los stakeholders de la organización de frente a la auditoría se convierte en relevante, permitiendo analizar o efectuar revisiones particulares de las excepciones obtenidas al universo de datos o grupos de información, generando valor para la organización en cuanto a:

- Calidad e integridad de la información: análisis de bases de datos, identificación de desviaciones según estructuras de datos y reglas de negocio.
- Cumplimiento regulatorio: establecer alertas para corroborar su cumplimiento (oportunidad en el otorgamiento de las prestaciones económicas, requisitos mínimos).
- Re-cálculos: establecer y comparar frente a re-cálculos (aplicación de fórmulas financieras determinadas).
- Cumplimiento de reglas de la operación: Identificación de desviaciones.
- Establecer tipo de prestación y causa: invalidez por tipos de enfermedad, centralización regional, por profesionales de la salud.
- Tiempos de respuesta a solicitudes por intermediarios registrados.
- Alteración de información en los sistemas para cometer fraudes a nivel de funcionarios.
- Pagos duplicados en un período.
- Controles de seguridad: micro-segmentación, virtualización de firewall, redes virtuales, control por aplicaciones, accesos por usuarios, acceso remoto.

La auditoría y su enfoque de valor

La auditoría hasta hace poco se encontraba en una zona que no tenía variaciones o cambios en sus alcances, debido a que las organizaciones no habían creado esas nuevas necesidades y el mundo exterior no había ingresado en plenitud en todos sus aspectos (financiero, económico, nuevos mercados, tecnologías nuevas, entre otros). Estos avances han propiciado que las compañías se vean enfrentadas a nuevos riesgos, que pueden ser visibles y afectan la operación, hasta situaciones que no se pueden detectar, como ataques cibernéticos; por tanto, el plan de auditoría interna debe ser confiable para detectar errores significativos, irregularidades y debilidades importantes en el control interno, pero no debe ser estático de un año al otro por cuanto debe ajustarse a los cambios en las actividades, mercados u otros aspectos del entorno externo de la organización que puedan incidir en los riesgos a los que ésta se enfrenta.

KPMG frente a las nuevas tendencias y necesidades en las organizaciones, ha generado un cambio con un esquema de auditoría donde ha innovado sus procesos, incorporando robótica o herramientas de análisis de datos, de tal manera que la función de auditoría mantenga el ritmo frente a los cambios acelerados en la tecnología, los retos del mercado y pueda ayudar a la organización a comprender y gestionar los riesgos asociados, logrando resultados esperados de la automatización y continuar innovando para agregar valor.

Para las administradoras de pensiones y el Estado, los cambios socioeconómicos y tecnológicos requieren de una auditoría que se encuentre a la vanguardia de estos cambios, con herramientas tecnológicas que permiten ser más precisos y tener un mayor cubrimiento, que generen un valor agregado a los servicios prestados, proporcionando conocimiento continuo sobre los

8 Decreto 726 de 2018 del Ministerio del Trabajo. Artículo 1. Modificación del Capítulo 2 del Título 9 de la Parte 2 del Libro 2 del Decreto 1833 de 2016.

9 KPMG ha incorporado con éxito el uso de tecnologías para el análisis de datos, como son Alteryx, Tableau, Qlik View, Quic Sense, Power BI; para análisis Forensic, Relativy, Nuix.

sistemas, procesos, controles y transacciones de las mismas, generando una mejora en la capacidad de supervisión sobre los riesgos y controles a través de la detección temprana y el monitoreo continuo. La auditoría debe proporcionar una mayor cobertura del universo auditado, análisis de poblaciones completas de datos y una mayor frecuencia de las mismas.

Enfocados en la complejidad del Sistema General de Pensiones, se busca un debido manejo y custodia de la información, por tanto las ventajas de una auditoría soportada en la tecnología, en un conocimiento profundo de los procesos, en el análisis de datos, y con una perspectiva de riesgos, permite tener un amplio alcance, generando valor en sus resultados para la organización; de acuerdo a las siguientes ventajas:

- Ahorro a partir de la eficiencia en los costos operativos, aportando una mayor cobertura por parte de la auditoría.
- Contar con indicadores constantes de rendimiento, generando más exactitud, transacciones procesadas y excepciones identificadas.
- Los robots de software no generan errores de cálculo permitiendo a la auditoría tener más exactitud. .
- La auditoría puede ser más oportuna con estos resultados actualizados para la organización, logrando generar una mejora continua, y los datos de rendimiento permiten identificar ajustes para mejorar y agilizar una tarea o proceso.
- Velocidad y eficiencia en los robots de software, por cuanto no descansan ni requieren períodos de adaptación, su capacidad de trabajo es 24 x 7 x 365, facilitando a la auditoria tener información actualizada para la identificación de posibles situaciones, desviaciones, tendencias o posibles riesgos.
- La capacidad de atención de los robots es ilimitada y sirve como herramienta de control para la auditoría.

Con estas ventajas la auditoría puede presentar informes más profundos, de mayor cobertura y entendimiento, presentando un análisis de extraordinario valor que permita estar más allá de un número, lo que generaría mayor confianza en la toma de decisiones, basados en la innovación y en el uso de la tecnología.

Transformar la auditoría a través de la tecnología y la innovación

En KPMG nos centramos en:

La tecnología como apalancador en la estrategia de aseguramiento de la organización.

Mantener un conocimiento continuo de los procesos.

Habilitar un nuevo enfoque y vista única del riesgo incluyendo un monitoreo permanente.

2.5 Auditoría de inversiones

Para hablar de auditoría de inversiones, debemos contemplar en primer lugar los factores de riesgos a los cuales se enfrenta y el papel que juegan la Gerencia de Riesgos con la auditoría de la organización en el proceso de inversiones, considerando su importancia estratégica de control y, teniendo como objetivos: identificar, evaluar, intervenir, prevenir, proteger, e informar situaciones de riesgo y monitorear mediante una metodología especializada acerca del cumplimiento a los objetivos estratégicos de la organización y la atención de todos sus grupos de interés.

En los últimos tiempos y como consecuencia de la globalización, el área de inversiones en las entidades ha venido creciendo y obteniendo una relevancia que ha hecho que su estructuración y diseño del proceso se haya venido realizando más concienzudamente, identificando los riesgos en cada una de las actividades para definir los controles que mitiguen los riesgos identificados.

Dentro de la experiencia obtenida en la evaluación del proceso de inversiones, los factores de riesgos críticos y a los cuales las entidades deben darle mayor importancia son:

- Riesgos regulatorios
- Riesgos financieros
- Riesgos legales y reputacional
- Riesgos de mercado (competencia)
- Riesgos de talento humano
- Riesgos asociados a la continuidad del negocio
- Seguridad de la información
- Riesgos asociados a fallas técnicas
- Riesgos de cumplimiento
- Riesgos asociados a la gestión del cambio o modelo de negocio

Por lo tanto las organizaciones que anticipen y definan rigurosamente dichos riesgos a los cuales están expuestas podrán darle fuerza al desempeño de su gestión y tomar ventajas.

Dentro de los factores determinantes para lograr el éxito en una organización, se encuentran la liquidez y la rentabilidad, relacionados al flujo de caja y el buen resultado de la gestión de inversión de los recursos respectivamente, ambos de la mano y vistos desde el área de inversiones se complementan para cumplir con la estrategia organizacional.

Para los auditores es de vital importancia que las organizaciones tengan claramente definidas los roles en las líneas de defensa de los actores del proceso de inversiones, teniendo claridad de sus funciones y responsabilidades.

El mercado de valores colombiano toma como lineamiento para la realización de sus procesos de auditoría lo dispuesto en el Decreto 2555 de 2010, normatividad que se ajusta a los estándares internacionales para la gestión y administración de activos del mercado de valores.

La normatividad es explícita en cuanto a las actividades y funciones de los diferentes actores del mercado, del proceso de inversiones, y en la administración de los recursos en cuanto a su estructura, instancias y segregación de funciones en las entidades vigiladas por el ente de control; de esta manera, la auditoría procede a validar las actividades de los procesos, el diseño y operatividad de los controles y lineamientos que nacen desde el primer nivel de la organización, actas de los comités de inversión y de riesgo, alineados a las disposiciones del decreto mencionado.

Por otra parte, las organizaciones del sector real, que no tienen una norma que las regule en este proceso de inversiones del mercado de valores, han venido desarrollando buenas prácticas tomadas de las entidades del sector financiero; en especial, la segregación de funciones de quién diseña y ejecuta la estrategia de inversión, quién controla los lineamientos y quién cumple las operaciones; deben ser áreas funcionales diferentes. Adicionalmente, estas entidades deben tomar como disciplina la definición de su apetito de riesgo para establecer los cupos de crédito y contraparte, límites a clase de títulos, operaciones permitidas y la rentabilidad objetivo.

Una vez descrito el contexto que cobija el proceso de inversiones de las entidades participantes en el mercado de valores, entraremos a exponer el rol que debe tener la auditoría en cada uno de sus frentes dadas las exigencias de la segregación de funciones en el proceso establecido por el ente de control, frentes que deben contar con los manuales de procedimientos, controles y políticas para mitigar los factores de riesgo asociados al proceso de inversiones en el Front, Middle y Back Office. Estas definiciones deben servir de base y mejores prácticas para la estructuración del área de inversiones en las entidades no reguladas.

Gráfica 18: Actores del proceso de inversión en los tres líneas de defensa

Fuente: KPMG construcción propia.

Dentro de las actividades que ejecuta la auditoría es importante incluir los siguientes aspectos con el fin de validar la adecuada gestión y administración de los recursos para cada una de las líneas de defensa, como se muestra en la gráfica 18.

Front Office

- Validar que la administradora de fondos y/u organización cuente con el personal idóneo calificado ante la AMV (Autorregulador del Mercado de Valores colombiano para gestionar los portafolios, para el sector financiero).
- Revisar que cuente con una estructura/organigrama, atribuciones y Comité de Inversiones mensual.
- Validar que el área cuente con herramientas y fuentes de información suficientes del mercado de valores para realizar análisis técnicos y fundamentales (entorno económico) para diseñar, evaluar, aprobar y ejecutar estrategias de inversión y establecer políticas para tomar decisiones de inversión o desinversión de los activos de los portafolios diariamente conforme al entorno económico, el costo de oportunidad del mercado y flujo de caja o necesidades de los fondos o portafolio propio.

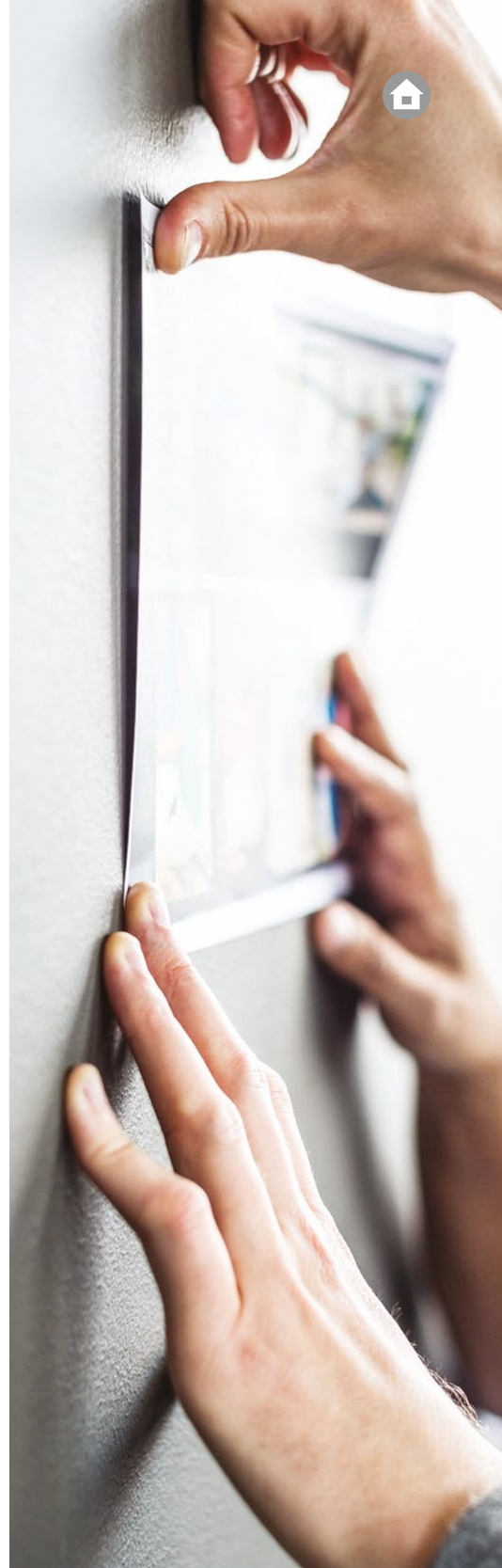
Igualmente, para la auditoría es relevante que sus equipos evalúen al interior de la entidad:

- El cumplimiento del benchmark o rentabilidad objetivo de los portafolios.
- La disponibilidad en tiempo real de los cupos, tanto de clase de títulos definidos en el régimen de inversión, emisor y contraparte, como el control sobre los mismos para no incurrir en incumplimientos.
- El conocimiento diario de la liquidez, vencimientos y flujo de adiciones y retiros de recursos que inciden en la misma.
- El ingreso a personal ajeno al área del Front Office.
- Y el acceso de celulares por parte del equipo operador dentro del espacio de negociación, el cual es prohibido en el sector financiero.

Middle Office

- Validar el control que ejerce el área de riesgos sobre el estricto cumplimiento de los manuales de políticas y procedimientos de inversión.

Monitorear indicadores financieros, factores de riesgo y su benchmark permite a los operadores del mercado identificar nuevas amenazas y oportunidades para los recursos administrados.



- Revisar el cumplimiento de los lineamientos de inversión y cupos establecidos.
- Validación de la valoración a precios de mercado.
- Efectuar re-cálculos y análisis de los diferentes riesgos a los cuales se enfrentan los portafolios.
- Revisar la implementación y cumplimiento del SARM y SARL conforme a lo estipulado por el ente de control para el sector financiero.

Back Office

- Validar la existencia de controles duales.
- Revisar los niveles de atribuciones y autorizaciones.
- Validar los niveles de acceso al master trader (sistema transaccional) para complementar y cumplir que no sea la misma persona.
- Evaluar el proceso referente al flujo de dinero para cumplir las operaciones o cuando se reciben recursos.
- Revisar el flujo de caja diario.
- Validar que se realicen arqueos de títulos mensuales y sorpresivos, que la cuenta en los depósitos de valores esté a nombre de la entidad (portafolio propio) o a nombre de los fondos administrados.
- Registro contable conforme a la normatividad vigente, dentro de los más relevantes.

Valor agregado de la auditoría Interna dentro de la organización

Con el fin de que el ejercicio de la auditoría brinde un valor agregado al proceso de inversiones, es relevante tener en cuenta:

- Ser un socio estratégico, dinámico y transversal de la entidad en los tres frentes.
- Promover oportunidades de mejora a los hallazgos encontrados.
- Generar valor agregado recomendando mejores prácticas para optimizar los procesos y políticas.
- Proveer información en el reporte de auditoría útil, relevante e importante para tomar decisiones; independiente, lo que incrementa su confiabilidad.
- Cumplir con las expectativas del auditado.

Las organizaciones que hoy mantienen su liderazgo han aprendido a proteger su nombre y obtener mejores resultados a través de la buena gestión del riesgo y con el apoyo de la auditoría, reconociendo la gran oportunidad que tienen para generar valor.

En medio de un ambiente cambiante normativo, del mismo mercado de valores afectado por el entorno económico y político, a la vanguardia de los avances tecnológicos y en la búsqueda del ente de control por consolidar el proceso bajo estándares internacionales, las organizaciones deben considerar a la auditoría como un socio estratégico, proactivo y transformador, donde su labor está encaminada a apoyar el perfeccionamiento del proceso, en respuesta a situaciones cambiantes, y a mitigar los riesgos que lo rodean en pro del beneficio de la organización de una manera más estratégica, sostenible e integrada.

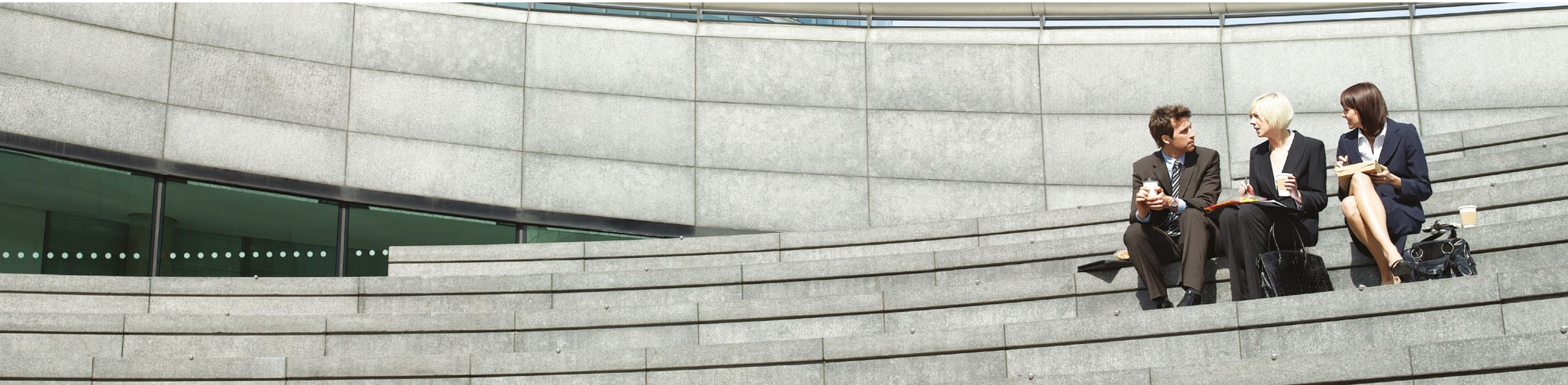
2.6 Auditorías externas de gestión y resultados

> Las auditorías externas de gestión y resultados, en adelante - AEGR, en Colombia están direccionadas para las entidades prestadoras de servicios públicos domiciliarios atendiendo lo definido en la Ley 142 de 1994 de servicios públicos, estas auditorías están reguladas por la Superintendencia de Servicios Públicos Domiciliarios, (SSPD), mediante la resolución 12295 del año 2006 que define su alcance y contenido, en ellas el auditor efectúa una revisión y análisis de indicadores de las compañías de servicios públicos domiciliarios con el propósito de evaluar su gestión interna teniendo en cuenta el objeto social, sus objetivos generales y su eficiencia como organización, con el fin de emitir un informe sobre la situación global del prestador.

El objetivo es atender los requerimientos consagrados en la Ley 142 de 1994, resolución 12295 de 2006 y demás normatividad, para las empresas de Servicios Públicos Domiciliarios, específicamente en:

- Evaluar la gestión del prestador de acuerdo con los criterios, metodologías, indicadores, parámetros y modelos que definan las comisiones y los requerimientos de la Superintendencia.
- Reportar a la SSPD los cambios significativos en la estructura organizacional.
- Verificar la conformidad de la gestión del prestador con los requisitos legales, técnicos, administrativos, financieros y contables del régimen de servicios públicos domiciliarios.
- Verificar la calidad de la información reportada por el prestador a través del Sistema Único de Información (SUI) para la emisión de los conceptos o determinación de cifras o indicadores solicitados por la SSPD.
- Asesorar en la identificación e informar oportunamente las situaciones que pongan en riesgo la viabilidad de las empresas.
- Identificar y valorar los riesgos que puedan afectar la prestación del servicio.
- Conceptuar sobre el estado de desarrollo del Sistema de Control Interno.
- Identificar e informar oportunamente las situaciones que pongan en riesgo la viabilidad de las organizaciones.
- Recomendar medidas correctivas, preventivas o de mejora.

Su alcance está determinado por el contenido de la resolución 12295 del año 2006 de la SSPD que establece el cumplimiento de ocho aspectos importantes dentro del cual se evalúa la gestión del prestador del servicio público domiciliario el cual incluye los siguientes capítulos:



Gráfica 19. Aspectos de cumplimiento Resolución 12295 de 2006

Fuente: KPMG construcción propia

Arquitectura organizacional

En relación con la información sobre arquitectura organizacional, el auditor deberá pronunciarse solo en aquellos casos en los cuales se hayan realizado cambios significativos con respecto al informe anterior teniendo en cuenta:

- La estructura organizacional actual.
- Cambios significativos en la estructura con respecto al período anterior.
- Actualización del Registro Único de Prestador del Servicio RUPS.
- Reporte del organigrama actual de la compañía.

Viabilidad financiera

El auditor deberá pronunciarse sobre la viabilidad financiera del prestador, por medio de la revisión del modelo suministrado por la organización, validando que dicha información esté alimentada con información básica financiera real de los dos (2) últimos años y conceptuar sobre los supuestos macroeconómicos (inflación, IPC, IPP, etc.) y los usados por el prestador para las proyecciones financieras cargadas al SUI (sistema único de información) en materia de flujo de caja, balance general y estado de resultados.

Se validarán entre otros los siguientes aspectos:

- Ingresos: evolución del mercado, demanda, tarifas o cambios en el marco tarifario y su impacto en los resultados financieros.
- Egresos: costos de producción, gastos administrativos, operacionales, reposición y mantenimiento de infraestructura y nuevas inversiones.

Así mismo, el auditor deberá conceptuar sobre la adecuada provisión y fondeo del pasivo pensional.

De igual manera se pronunciará sobre las metas establecidas en los planes de gestión, resultados y el nivel de cumplimiento de los mismos en relación con sus proyecciones financieras y las situaciones que pongan en peligro la viabilidad financiera del prestador.

Análisis de puntos específicos

El auditor deberá presentar un análisis y evaluación, que incluya sus opiniones y recomendaciones, respecto a:

- La gestión financiera.
- La gestión técnica y operativa.
- La gestión comercial.
- La gestión legal.

De todos los puntos que se relacionan el auditor deberá realizar un análisis detallado del cumplimiento de los programas de gestión y/o acuerdos de mejoramiento suscritos con la SSPD. Así mismo, el auditor podrá incluir en este punto análisis complementarios a efectos de dar claridad sobre los temas solicitados y que considere deben ser conocidos por el ente regulador.

3.1 Gestión financiera

En este capítulo el auditor incluirá la gestión del prestador en la administración y manejo de los recursos financieros relacionados con la operación del servicio.

El auditor deberá verificar que la información financiera, contable y de costos cargada al SUI, esté elaborada con base en lo establecido en las Resoluciones SSPD 1416 y 1417 de 1997, para el reporte del año evaluado 2005, y la Resolución SSPD 2005-1300033635 del 28 de diciembre de 2005 para los reportes a partir del año evaluado 2006, y las normas que las sustituyan, deroguen o modifiquen.

A su vez, deberá expresarse sobre si los estados financieros cargados por el prestador al SUI corresponden a estados financieros debidamente certificados, así como dictaminados y si las opiniones del revisor han sido tenidas en cuenta por el prestador.

De igual forma, la AEGR deberá dar su concepto sobre los costos laborales y analizar el impacto en el factor prestacional de la convención colectiva si esta existiese.

El análisis financiero de este capítulo se apoyará en los indicadores de: liquidez, solvencia, rentabilidad, endeudamiento y causal de disolución.

3.2 Gestión técnica y operativa

Incluye la gestión en la inversión, operación, mantenimiento y seguridad de la infraestructura asociada a cada servicio, así como aspectos y condiciones de cobertura, disponibilidad, confiabilidad, continuidad y oportunidad con las que se presta el servicio público, con base en lo establecido en la regulación para cada sector. Por ejemplo, en el sector Energía y Gas se incluyen los siguientes puntos de atención sobre los cuales el auditor debe enfocar su análisis y cumplimiento de la gestión:

- Mantenimiento en redes y equipos, inversión.
- Cumplimiento normativo.
- Calidad en construcción, seguridad de redes e instalación del usuario.
- Procedimiento de detección de violaciones al CCU y medición de índices de calidad.
- Respuesta al servicio técnico, interrupciones y presiones en líneas individuales, odorización.
- Pago de compensaciones generadas al usuario por los incumplimientos presentados.

3.3 Gestión comercial

El auditor deberá incluir el análisis de la gestión de medición, facturación y cobro del servicio, así como las actividades que adelanta el prestador para atender las peticiones y reclamaciones de los usuarios del servicio, teniendo en cuenta aspectos logísticos, procedimentales y demás que puedan afectar la relación usuario-prestador, con base en lo establecido en la regulación para cada sector. Un caso de ejemplo, puede ser para el sector de Energía y Gas sobre los siguientes puntos de atención en los cuales el auditor debe enfocar su análisis y cumplimiento de la gestión:

- Nivel de pérdidas, recaudo y cartera, facturación, tarifas subsidios y contribuciones.
- Puntos de atención, y tiempos de atención en oficinas y de la correspondencia.
- Nivel de satisfacción del usuario, tiempo de conexión y reconexión al usuario.

3.4 Gestión legal

Aquellos factores exógenos que pueden afectar la prestación de los servicios públicos domiciliarios sobre los cuales el auditor deberá dar su análisis y conceptos de acuerdo a lo siguiente:

- Naturales (climatológicos, desastres, etc.). Precios de combustibles.
- Regulatorios (Normas CREG, MME, SSPD, etc.), legales (demandas, sanciones, etc.).
- Intervención por parte de la SSPD.

Indicadores y referentes de la evaluación de gestión

El auditor deberá efectuar el cálculo de los indicadores y referentes los cuales están compuestos dependiendo del sector del servicio público (agua, energía, gas) de cinco indicadores financieros y técnicos; para ejemplificar incluimos los indicadores del sector de gas, en la tabla 4.

Tabla 4: Indicadores y referentes de gestión

Indicador	Fórmula
Rotación cuentas por cobrar (días)	Rotación cuentas por cobrar $= \left(\frac{\text{Cuentas por cobrar}}{\text{Ingresos operacionales}}\right) * 365$
Rotación cuentas por pagar (días)	Rotación cuentas por pagar $= \left(\frac{\text{Cuentas por pagar}}{\text{Costo de ventas}}\right) * 365$
Razón Corriente (veces)	Rotación corriente $= \frac{\text{Activo corriente}}{\text{Pasivo corriente}}$
Margen operacional (%)	Margen operacional $= \left(\frac{\text{EBITDA}}{\text{Ingresos operacionales}}\right) * 100$
Cubrimiento gastos financieros (veces)	Cubrimiento de gastos financieros $= \frac{\text{EBITDA}}{\text{Gastos finacieros}}$
Suscriptores sin medición (%)	Suscriptores sin medición $= \left(\frac{\text{Suscriptores sin medición}}{\text{Suscriptores totales}}\right) * 100$
Cobertura (%)	Cobertura $= \frac{\text{Suscriptores}}{\text{Suscriptores en contrato}} * 100$
Reclamos facturación (por 10,000)	Relación reclamos facturación $= \left(\frac{\text{Reclamos facturación}}{\text{Facturas expedidas}}\right) * 10.000$
Atención reclamos servicio (%)	Atención reclamos servicio $= \left(\frac{\text{Usuarios afectados}}{\text{total usuarios}}\right) * 100$
Atención solicitud conexión (%)	Atención solicitud conexión $= \left(\frac{\text{Usuarios afectados}}{\text{total usuarios}}\right) * 100$

Fuente: KPMG construcción propia a partir de la información contenida en la resolución 12295 de SSPD

Concepto de la AEGR

El auditor deberá dar su opinión sobre cada uno de los indicadores respecto de las desviaciones positivas o negativas frente a los referentes del año y su razonabilidad de acuerdo con las condiciones comerciales, técnicas, financieras y administrativas en las que se presta el servicio y sobre la evolución del resultado de los indicadores durante los últimos 4 años, incluido el año evaluado.

Indicadores nivel de riesgo

El auditor deberá efectuar el cálculo de los indicadores de nivel de riesgos los cuales están diseñados para todos los sectores que prestan servicios públicos (agua, energía, gas), en su totalidad son financieros y se elaboran partiendo de los estados financieros dictaminados por el revisor Fiscal de la Compañía. A continuación presentamos la estructura de los indicadores:

Tabla 5 Indicadores nivel de riesgo

Indicadores clasificación por nivel de riesgo	
Indicador	**Fórmula**
Período de pago del pasivo de largo plazo (años)	Periodo de pago pasivo LP $= \frac{\text{Pasivo total - Pasivo corriente}}{\text{EBITDA - Impuesto de renta}}$
Rentabilidad sobre activos (%)	Rentabilidad sobre activos $= \left(\frac{\text{EBITDA}}{\text{Activo total}}\right) 100$
Rentabilidad sobre patrimonio (%)	Rentabilidad sobre patrimonio $= \left(\frac{\text{Gastos impuesto}}{\text{EBITDA - Financieros - de renta}}{\text{Activo Total}}\right) * 100$
Rotación activos fijos (veces)	Rotación activos fijos $= \frac{\text{Ingresos operacionales}}{\text{Activo fijo}}$
Capital de trabajo sobre activos	Capital de trabajo sobre activos $= \left(\frac{\text{Capital de trabajo}}{\text{Activo total}}\right) * 100$
Servicio de deuda sobre patrimonio	Servicio de deuda sobre patrimonio $= \left(\frac{\text{Servicio de deuda}}{\text{Patrimonio}}\right) * 100$
Flujo de caja sobre servicio de deuda	Flujo de caja sobre servicio de deuda $= \left(\frac{\text{Flujo de caja}}{\text{Servicio de deuda}}\right) * 100$
Flujo de caja sobre activos	Flujo de caja sobre activos $= \left(\frac{\text{Flujo de caja}}{\text{Activo total}}\right) * 100$
Ciclo operacional	Ciclo operacional = Rotación cxc - Rotación cxp
Patrimonio sobre activo	Patrimonio sobre activo $= \left(\frac{\text{Patrimonio}}{\text{activo total}}\right) * 100$
Pasivo corriente sobre pasivo total	Pasivo corriente sobre pasivo total $= \left(\frac{\text{Pasivo corriente}}{\text{pasivo total}}\right) * 100$
Activo corriente sobre activo total	Activo corriente $= \left(\frac{\text{Activo corriente}}{\text{Activo total}}\right) * 100$

Fuente: KPMG construcción propia a partir de la Resolución 12295 de la SSPD

Información reportada al SUI

El auditor deberá conceptuar sobre la calidad de la información reportada por el prestador al SUI y utilizada por ella para la emisión de los conceptos o determinación de cifras sobre los indicadores de riesgo solicitados, indicando si la información cargada por el prestador refleja la realidad de la empresa. Este concepto será registrado por el auditor en los formularios que se dispondrán para el reporte que se envían a través del Sistema Único de Información de la SSPD.

Matriz de riesgos

El auditor identificará los riesgos asociados a cada uno de los procesos que se establecen según el sector y posteriormente deberá establecer su probabilidad de ocurrencia e impacto con el objeto de determinar el riesgo del proceso de acuerdo con las definiciones que se presentan en la resolución 12295. En el caso de que la AEGR identifique riesgos en otros procesos no especificados, deberá adicionar el nombre correspondiente al proceso y pronunciarse de la misma manera.

Así mismo, deberá indicar los controles que la empresa ha diseñado o implementado para minimizar los riesgos. Esta evaluación depende del buen juicio, experiencia y conocimiento del auditor y del uso de las herramientas que considere necesarias. La Matriz de Riesgos se presentará en un archivo plano en formato de valores delimitado por comas (Comma Separated Values -CSV) que cumple con las especificaciones dadas por el SUI; debe contener: macroproceso, proceso, riesgo, probabilidad de ocurrencia, magnitud del impacto, control; estos elementos están explicados en la Resolución 12295.

Evaluación sistema de control interno

El auditor o el jefe de la oficina de control Interno del prestador o quien haga sus veces deberá realizar un diagnóstico que determine el estado general y grado de desarrollo del sistema de control interno y de los elementos que lo conforman como instrumento de control empresarial. A partir de los hallazgos del diagnóstico presentará recomendaciones sobre las acciones correctivas y/o de mejoramiento requeridas para mejorar el sistema de control interno.

Para cumplir con el anterior objetivo, la AEGR o el jefe de control interno, según sea el caso, debe contestar de manera objetiva manteniendo siempre la coherencia entre las respuestas que se registren y la situación real observada por el auditor, la encuesta de control interno que se detalla en la resolución 12295, cuyo alcance cubre los subsistemas, componentes y elementos del sistema como son el subsistema de control estratégico y el subsistema de control de gestión.

El concepto general sobre el grado de desarrollo del sistema de control interno y las recomendaciones sobre las acciones correctivas y/o de mejoramiento que sean viables implementar para el prestador, deberá ser remitido por la AEGR a través de la página web www.sui.gov.co en formato PDF.

2.7 Auditoría interna y los riesgos de ciberseguridad

Dado el creciente número de ciberataques y violaciones de datos de alto perfil, las organizaciones de todos los sectores le han dado un lugar privilegiado a la seguridad cibernética en la agenda de la Junta Directiva como prioridad para el logro de sus objetivos empresariales.

Los costos asociados a estos sucesos, han llegado a ser tan significativos que las organizaciones están centrando su atención en cómo proteger sus activos, en especial las organizaciones que tratan con datos sensibles, como información personal, datos bancarios o de titulares de tarjetas, información financiera de la empresa, propiedad intelectual o información material no pública.

Aunque los graves riesgos involucrados han puesto a las organizaciones en alerta, muchas no se sienten preparadas. Según el informe de 2018 de Harvey Nash/KPMG CIO Survey, sólo el 22% de los líderes de TI sienten que están "muy bien preparados" para defenderse de un ciberataque; sin embargo, el 68% de los líderes de TI consideran que cuentan con el apoyo necesario de la alta dirección para alcanzar sus objetivos de ciberseguridad. Por lo tanto, con el creciente apoyo del liderazgo ejecutivo ¿cómo pueden las organizaciones y sus funciones de auditoría interna cerrar la brecha en la preparación para la seguridad cibernética?

Lo primero es entender qué es una violación de datos, que generalmente se define como un evento en el que los datos sensibles o confidenciales son copiados, vistos, robados o utilizados por una persona o entidad no autorizada para hacerlo. Las actividades que contribuyen a la violación de datos u otras formas de ciberdelincuencia incluyen el error humano, la intención política o criminal, las tecnologías emergentes o el cambio empresarial, entre otros.

Los malos "actores" de ayer han evolucionado desde criminales aislados o los "script kiddies" que apuntan al robo de identidad, oportunidades de autopromoción o robo de servicios, a los delincuentes organizados de hoy en día, los estados nacionales, los activistas o las personas con información privilegiada que se centran en la propiedad intelectual, la información financiera o el acceso estratégico a los recursos clave. Según el reporte de Cyxtera Technologies "The Fraud Beat 2018" en el que se investigaron los ataques más sofisticados que afectan tanto a las organizaciones, como a los consumidores e instituciones financieras alrededor del mundo, las amenazas para explotar los sistemas incluyen, los ataques de suplantación de identidad (phishing), señalando que el 90% de los ejecutivos de ciberseguridad mencionan que han sido blanco de ataques entre 2017 y 2018; para el 2020 el 60% de las compañías habrán sido víctimas de phishing y el 40% de los emails de spam reportados, son en realidad ataques de phising; el malware de rescate (ransomware), con un incremento del 229% en el número de ataques entre el 2017 y 2018; troyanos bancarios, en promedio más de 200 instituciones financieras a nivel mundial han sido afectadas por el troyano Trickbot; redes sociales, violaciones de datos, afectación de emails corporativos, inteligencia artificial y hackeo de elecciones.

Por su parte, el estudio del costo de la violación de datos 2018: Global Overview realizado por Ponemon Institute LLC y patrocinado por IBM Security, en el que se entrevistaron 2.200 profesionales de TI, de protección de datos y de cumplimiento de 477 compañías que han experimentado una violación de datos en los últimos 12 meses, señala que éstas siguen siendo muy costosas para las organizaciones y resultan en la pérdida o robo de registros de consumidores. El estudio revela que el costo total promedio de una violación de datos es de US$3,86 millones, cifra que aumenta por año en un 6,4%. El costo promedio de cada registro perdido o robado es de US$148 mientras que en el 2017 fue de US$141. De igual manera continua señalando el estudio, que la probabilidad de una violación recurrente en los próximos 2 años es de 27,9%, y los factores para determinarla fueron: el tamaño de la violación de datos reportada en la investigación y dónde se localiza la organización, siendo Sudáfrica el país con mayor probabilidad de experimentar una violación de datos, con un 43% y Alemania el de menor probabilidad con un 14,3%.

> Al igual que en años anteriores, el estudio informa sobre la relación entre la rapidez con que una organización puede identificar y contener una violación de datos y las consecuencias financieras, y señala que el tiempo medio de identificación fue de 197 días y el tiempo promedio para contener la violación fue de 69 días. Las organizaciones que lograron contener una violación en menos de 30 días ahorraron más de un US$ 1 millón en comparación con las que tomaron más de 30 días. Los ataques maliciosos o criminales causan la mayoría de las violaciones consolidadas en el estudio con un 48%, seguida por errores humanos con un 27% mientras que el 25% de las violaciones involucró fallas en los sistemas incluidos procesos empresariales y de TI.

En Colombia, el Centro Cibernético Policial (CCP), es la dependencia de la Dirección de Investigación Criminal e INTERPOL, responsable de liderar los esfuerzos institucionales para enfrentar la amenaza del Cibercrimen y Ciberterrorismo. Como afirma el T.C. Durán (2019), en las principales amenazas globales están, el ransomware y la ingeniería social, tal como lo menciona Cyxtera Technologies, los ataques de denegación del servicio focalizados, el fraude en medios de pago con tarjeta no presente (skimming), el criptojaking, la dark web, entre otras, e indica que en 2017 se presentaron en Colombia 15.942 denuncias de cibercrimen, cifra que se incrementó en un 36% para el 2018, con 21.687 denuncias, de las cuales el 60% se concentra en las ciudades de Bogotá, Medellín, Cali, Bucaramanga y Barranquilla. El delito de mayor afectación a nivel nacional es el hurto por medios informáticos y semejantes, que incluye el acceso abusivo a sistemas de información, violación de datos personales, transferencia no consentida de activos y suplantación de sitios web, con 12.014 casos en 2018; el ransomware y los correos electrónicos comprometidos (BEC por sus siglas en inglés, Business Email Compromise), representan una prioridad en el proceso investigativo que adelanta el CCP.

De igual manera continúa señalando que los sectores de mayor afectación por incidentes cibernéticos son la ciudadanía en general con el 56% y el sector financiero con el 22% e indica que se reciben hasta 60 denuncias diarias de delitos informáticos en Colombia.

A medida que los ciberataques se vuelven más sofisticados, la supervisión por parte de la Junta Directiva al plan de respuesta cibernética de una organización ya no es una buena práctica, sino que se ha convertido en un requisito mandatorio. En este contexto, es pertinente retomar la pregunta antes formulada ¿Cómo puede la auditoría interna evaluar los riesgos de la ciberseguridad?

Para responder este interrogante, es pertinente mencionar que las funciones de auditoría interna pueden ejecutar una variedad de evaluaciones técnicas y de procesos para ayudar a identificar, evaluar y mitigar los riesgos de ciberseguridad. La gráfica 20 proporciona una guía de actividades importantes que la función de auditoría interna debería ejecutar, así como ejemplos de los elementos del alcance que podría considerar.

Gráfica 20. Evaluaciones técnicas de procesos y controles de ciberseguridad - Auditoría Interna

Evaluaciones técnicas	
Operaciones y tecnología	Análisis de vulnerabilidades y pruebas de penetración
	Acceso a la red y monitoreo / evaluación de amenazas
	Revisiones de configuración de dispositivos (infraestructura, firewalls, routers, etc.)
	Wi-Fi: configuraciones y pruebas de vulnerabilidades / explotación Wi-Fi no autorizado
	Puntos de acceso remoto / VPN: evaluación técnica de los puntos de acceso remoto y de la configuración para ayudar a garantizar su protección
	Evaluación de aplicaciones / bases de datos, por ejemplo, análisis de vulnerabilidades, pruebas de penetración y configuración de bases de datos
	Seguridad por diseño
	Revisiones y análisis de arquitectura
	Configuración de seguridad del sistema operativo / base de datos
	Proceso de parcheo / procedimientos de reparación
	Revisión de código

Gráfica 20. Evaluaciones técnicas de procesos y controles de ciberseguridad - Auditoría Interna

Evaluaciones de procesos y controles	
Operaciones y tecnología	Gestión de identidades y accesos: • Centralización vs. descentralización • Inicio de sesión único / Single sign-on • Procedimientos de gestión de acceso • Gestión de acceso remoto y autenticación • Gestión de acceso privilegiado
	Seguridad física y personal: • Controles de acceso lógico y físico • Conciencia de seguridad / ingeniería social
	Seguridad de los dispositivos móviles
	Evaluaciones de seguridad de las operaciones
Factores humanos	Gestión del talento y formación en TI
Dirección y gobierno	Gobierno de ciberseguridad, funciones y responsabilidades
	Integración de la gestión de riesgos cibernéticos y empresariales
Legal y cumplimiento	Consideraciones reglamentarias e integración en el marco cibernético
Gestión de riesgos de la información	Gestión de riesgos de los proveedores y seguridad
	Análisis de amenazas cibernéticas y proceso de gestión de riesgos: • Identificación de amenazas, evaluación y proceso de actualización • Gestión del cambios, incluida su integración en el ciclo de vida de desarrollo de software
	Seguridad informática en la nube y evaluación continua
	Clasificación, protección y cifrado de datos, programas de formación y sensibilización en toda la organización
Continuidad del negocio y gestión de crisis	Respuesta a incidentes de seguridad y comunicación: • Plan de comunicación de crisis • Funciones y responsabilidades del equipo • Procedimientos de notificación (legales, regulatorios, etc.) • Proceso de cierre • Controles durante un incidente • Investigación • Formación y sensibilización
	Integración con la seguridad
	Recuperación ante los desastres / resiliencia
	Proceso de evaluación del impacto empresarial
	Estrategia de prueba

Fuente: "The role of internal audit in cyber security readiness" de KPMG publicado en 2019

Factores de riesgo cibernético que la auditoría interna debe tener en cuenta

> Muchas organizaciones creen que están adecuadamente protegidas puesto que realizan pruebas de penetración periódicas o cuentan con las mejores herramientas técnicas de su clase. Sin embargo, los límites de la participación para combatir a los ciberdelincuentes y minimizar el riesgo de violaciones de datos se están ampliando para incluir procesos operativos y áreas como las que se mencionan a continuación:

Amenazas emergentes

El panorama de las amenazas cibernéticas cambia continuamente y evoluciona. La mayoría de los equipos de defensa cibernética dentro de una organización intentan abordar y mitigar el entorno de amenazas emergentes a través de una combinación de controles y técnicas. Por ejemplo, las organizaciones confían en los proveedores de información sobre amenazas basados en suscripciones para proporcionar actualizaciones en tiempo real sobre las amenazas nuevas y emergentes que prevalecen en un momento dado. Además, las organizaciones pueden realizar su propio reconocimiento investigando y accediendo a portales de discusión de medios sociales conocidos. Esta inteligencia es luego aplicada en planes de remediación y controles preventivos.

Por ejemplo, una organización fue informada de un ataque inminente de denegación de servicio a menos que se cumplieran ciertas condiciones de rescate. La organización respondió inmediatamente con controles adicionales en torno a su enfoque de mitigación de la denegación de servicio, así como con una mayor supervisión de los sistemas potencialmente afectados.

La Security Exchange Commission (SEC) publicó recientemente un informe de investigación para que las organizaciones tomen conciencia de que existen amenazas de comunicaciones electrónicas fraudulentas relacionadas con la cibernética y que deben ser consideradas en los sistema de controles internos. Las investigaciones de la SEC se centraron en las "comunicaciones electrónicas fraudulentas" o "afectación de correos electrónicos corporativos" (BEC por sus siglas en ingles) en los cuales los perpetradores se hicieron pasar por ejecutivos o vendedores de la compañía y usaron correos electrónicos para engañar al personal de la compañía y enviar grandes sumas a cuentas bancarias controladas por los perpetradores. Los fraudes en algunos casos duraron meses y se detectaron después de la intervención de la policía o de terceros. Cada una de las compañías perdió al menos US$ 1 millón, dos perdieron más de US$ 30 millones y una perdió más de US$ 45

millones. En total, las nueve compañías transfirieron casi US$ 100 millones como resultado de los fraudes, la mayoría de los cuales no se pudieron recuperar.

La auditoría interna debe evaluar la estrategia general de la organización para hacer frente a las amenazas emergentes desde una perspectiva de gobierno, arquitectura, operaciones y tecnología. Las organizaciones líderes en la práctica tendrán un enfoque bien definido para hacer frente al nuevo entorno de amenazas emergentes.

Cambio tecnológico

El ritmo actual del cambio que afecta a las organizaciones hoy en día con respecto a la innovación tecnológica va en aumento. Las organizaciones, después de muchos años, están incrementando su gasto en nuevas tecnologías para lograr en sus negocios un ritmo de crecimiento cada vez mayor. La adopción de la nube, el aumento de la demanda de automatización inteligente, la robótica y el auge de la Internet de las Cosas (IoT por sus siglas en inglés) han añadido nuevos y más complejos riesgos de seguridad al entorno empresarial.

La auditoría interna se enfrentará al reto de evaluar los riesgos cibernéticos de estas tecnologías nuevas y emergentes. Será importante evaluar el riesgo empresarial actual asociado al cambio tecnológico en términos de su impacto en las organizaciones.

Además, se debe considerar la posibilidad de tener en cuenta las nuevas iniciativas que podrían introducir riesgos en la organización como resultado de las tecnologías emergentes. Sería conveniente que la auditoría interna se preguntara si ¿ha adoptado la organización los principios de "seguridad por diseño" y está llevando a cabo revisiones de diseño o de tecnología antes de la adopción e implementación final de la tecnología? y la ejecución de su plan de auditoría debería responder estos interrogantes.

Cambio de negocio

El cambio empresarial se ve afectado por el cambio tecnológico, los cambios en el entorno normativo, los nuevos modelos empresariales y el impacto de las fusiones, adquisiciones o desinversiones.

Tradicionalmente, las funciones de auditoría interna han sido proactivas a la hora de abordar el riesgo empresarial asociado a estos cambios. Sin embargo, hasta hace poco, la consideración del riesgo cibernético y su impacto asociado no siempre ha sido considerada en la profundidad y amplitud que debería ser.

Los principales riesgos cibernéticos que deben tenerse en cuenta son, los relacionados con el entorno de amenaza de la organización y el riesgo cibernético de fusiones y adquisiciones para la entidad adquirente. Por ejemplo, si una organización se encuentra en modo de adquisición, la evaluación del riesgo cibernético y el impacto de las violaciones de datos conocidos deberían formar parte de la evaluación de la debida diligencia.

Cambios regulatorios

En todas las industrias, el cambiante panorama regulatorio tiene un impacto en la organización. La reciente legislación de General Data Protection Regulation (GDPR) y otras leyes y requisitos de seguridad de datos y privacidad, tales como los requisitos del New York Department of Financial Services (NYDFS), han impuesto requisitos adicionales de control a las organizaciones. Algunas organizaciones no han estado tan preparadas para abordar estos nuevos requisitos reglamentarios por lo cual se han abierto a la posibilidad de sanciones o multas reglamentarias.

Además, en el informe de prioridades de examen de 2019, publicado recientemente por la SEC, la ciberseguridad se destacó como una prioridad en los cinco programas de examen de la Office of Compliance Inspections and Examinations (OCIE). Estos exámenes se centrarán en las configuraciones, los dispositivos de almacenamiento en red, el gobierno de la seguridad de la información y las políticas y procedimientos relacionados con la seguridad de la información. La SEC también mencionó que hará hincapié en las organizaciones con múltiples oficinas, fusiones recientes y otras áreas tales como evaluaciones de riesgo, controles de acceso, prevención de pérdida de datos y más. No sería extraño que otros organismos de supervisión internacionales o nacionales, tomaran uno o varios de los aspectos antes mencionados para realizar sus revisiones o auditorías, y valdría la pena que las organizaciones estuvieran preparadas para atender los requerimientos del órgano de control que corresponda.

La auditoría interna puede desempeñar un papel clave en la evaluación del impacto de los reglamentos nuevos o existentes, así como en la evaluación del grado de preparación de su organización para lidiar con la nueva regulación.

Riesgo de terceros

La mayoría de las organizaciones tienen una cadena de suministro cada vez más compleja y han aumentado su dependencia de proveedores externos para que proporcionen bienes y servicios a su organización. Esta mayor dependencia ha aumentado el riesgo cibernético al permitir que terceros accedan a sus sistemas directamente o a través del procesamiento de su información privada o confidencial o de la de sus clientes. Todas las industrias deben tener un manejo sólido de la naturaleza de la información que está siendo utilizada por el tercero, cómo se transmite la información y cómo es almacenada y procesada. En muchos casos, una cuarta parte puede estar involucrada. La auditoría interna puede realizar evaluaciones de terceros, como parte de su plan de auditoría, así como evaluaciones detalladas de los proveedores de alto riesgo.

La participación de la auditoría interna en la preparación para la seguridad cibernética, será diferente para cada organización, al igual que las amenazas a las que esta última se enfrenta. En consecuencia, cada estrategia de respuesta cibernética será diferente.

Sin embargo, para las funciones de auditoría interna, existen algunas áreas comunes de enfoque ante las amenazas de ciberseguridad que deben ser consideradas al momento de determinar el alcance del plan de auditoría en esta área. La gráfica 21, proporciona un ejemplo.

Se necesita una comprensión integral de la organización, sus objetivos, sus riesgos y sus procesos para poder abordar completamente los desafíos de ciberseguridad que una organización puede enfrentar en la actualidad. La auditoría interna debe estudiar a fondo su organización, y poseer un sólido conocimiento técnico para alinear la ejecución de sus procesos con los objetivos organizacionales.

Elegir el enfoque correcto para evaluar su programa de ciberseguridad puede ser un desafío, especialmente porque el talento cibernético cualificado sigue siendo un reto para muchas funciones de auditoría interna.

Gráfica 21. Áreas comunes de enfoque ante amenazas de ciberseguridad – Plan de auditoría interna

Fuente: "The role of internal audit in cyber security readiness" de KPMG publicado en 2019

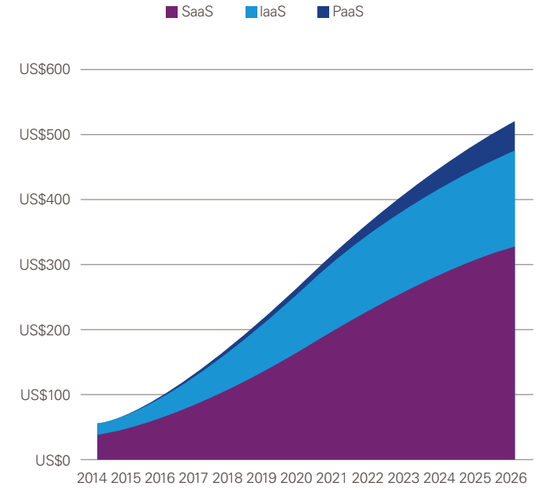
2.8 Riesgos y controles en cloud computing

Como parte de una tendencia global con sus ventajas y desventajas, pretendemos compartir el entendimiento de los principales riesgos y controles de este tipo de ambiente. Es importante conocerlos para permitir mejor implementaciones controladas en cualquier tipo de organización.

El ecosistema de la nube está madurando y escalando rápidamente para responder a la aceleración de la economía digital. Las soluciones IaaS, PaaS y SaaS permiten que la organización sea más autosuficiente, reduciendo la demanda de tecnología tradicional y liberando recursos para trabajar en iniciativas más complejas y de mayor valor. En la gráfica 22 se muestran las tendencias de estas plataformas utilizadas.

Gráfica 22: Tendencia de uso de plataformas

Ingresos de la nube pública mundial, 2014 - 2026 por SaaS, PaaS, and IaaS[10]

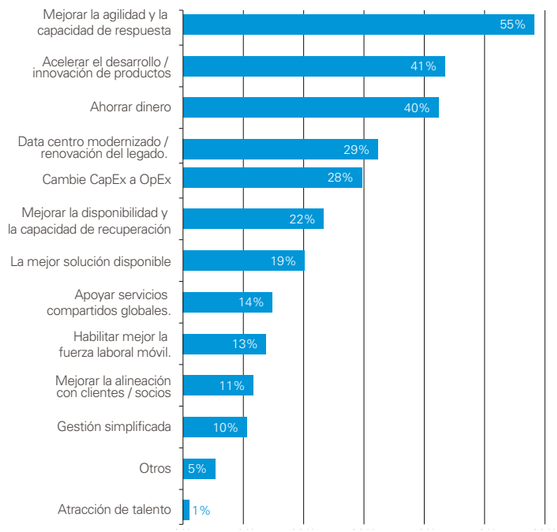


Fuente: *Wikibon 2016*

Este crecimiento está respaldado por algunos estudios que nos muestran cifras a considerar como:

- Se puede ver que la inversión en tecnología Cloud y el cambio a estas plataformas está aumentando considerablemente, por ejemplo, en la encuesta anual "CIO SURVEY 2018" realizado por KPMG y Harvey Nash, el 52% de los líderes digitales ha invertido en soluciones en la nube. Ver gráfica 23.
- Así mismo, en el informe de amenazas a la nube 2019 realizado entre KPMG y Oracle Cloud, se identifica que para el año 2020 el 49% de los encuestados contarán con sus datos en la nube.

Gráfica 23. Resultados encuesta anual CIO SURVEY 2018 KPMG – Harvey Nash

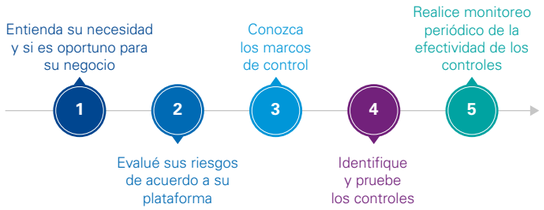


Fuente: Harvey Nash / KPMG 2016 CIO Survey

Como todo lo nuevo, siempre trae dudas para las organizaciones a la hora de tomar la decisión de entrar en esta tendencia. Llevar los riesgos a nivel cero siempre será imposible pero es importante entender cuáles pueden ser, cómo clasificarlos y saber que existen diferentes marcos de control que ayudan a conocer las diferentes contramedidas. Nuestro objetivo es brindar una guía práctica de cinco pasos para abordar con mayor tranquilidad en cualquier organización sin importar el tamaño o industria la computación en la nube (Cloud Computing). La metodología propuesta se resume en la Gráfica 24.

10 SaaS: Software como un Servicio; PaaS: Plataforma como un servicio; IaaS: Infraestructura como un Servicio

Gráfica 24. Metodología propuesta



Fuente: KPMG construcción propia

1. Entienda su necesidad y si es oportuno para su negocio

Antes de iniciar cualquier implementación es muy importante tener los conceptos claros en cuanto a los tipos de modelos de servicio que puede ofrecernos la Nube (Gráfica 25).

Adicionalmente, los modelos de entrega son: privada, comunitaria, pública e hibrida.

Después de tener esta claridad, se deben entender los beneficios y no ver la nube como un simple proyecto sino como una estrategia de negocio con un alto componente tecnológico. El éxito de una implementación se logra cuando los patrocinadores (alta gerencia) logran entender los beneficios para el negocio.

- ¿El grupo de alta gerencia tiene como visión estratégica Cloud Computing? ¿Su implementación generará valor? ¿Se tienen los costos de oportunidad identificados?
- ¿Cómo los planes de cloud computing soportan la estrategia de negocio?
- ¿Se ha evaluado si la organización está preparada? procesos, cultura, conocimientos, habilidades, estructura, entre otros.
- ¿Se tiene contemplado que las inversiones a realizar se pueden perder? Se tiene contemplado como se administrará el cambio en cuanto a:
  - Procesos.
  - Cultura y comportamientos.
  - Servicios, infraestructura y aplicaciones.
  - Habilidades y competencias.
- ¿Se tiene claridad cómo se medirá el retorno de la inversión vs los riesgos con los objetivos del negocio? ¿Se obtuvieron los beneficios esperados?

No se deje llevar por la tendencia ni por la presión de los terceros (implementadores o proveedores de software o hardware). Resuelva las cinco (5) preguntas anteriores y si está tranquilo con las respuestas va por buen camino, de lo contrario, realice el diagnóstico de su situación y establezca los planes para llegar al camino deseado.

Gráfica 25. Modelo tradicional vs modelo de cloud computing

Modelo tradicional	Modelo de cloud computing
Software	Software como un servicio (SaaS)
Middleware	Plataforma como un servicio (PaaS)
Sistema operativo	Infraestructura como un servicio (IaaS)

Fuente: KPMG construcción propia

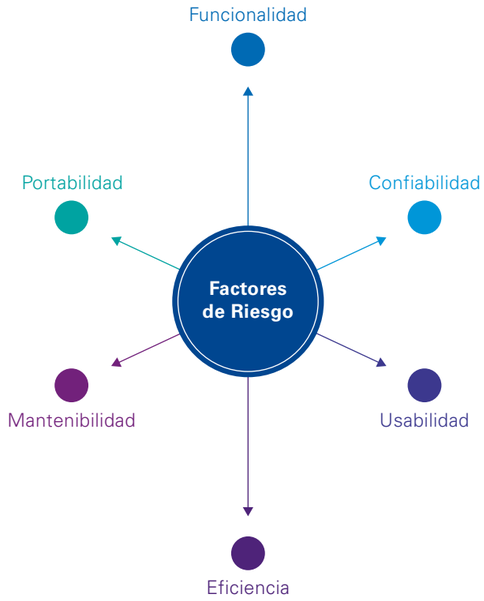
2. Evalué sus riesgos de acuerdo a su plataforma

Antes de iniciar con los riesgos es importante recordar los retos que trae la nube.

a. Información disponible y estar seguro que los planes de continuidad operan.
b. Claridad sobre los temas legales y de impuestos de acuerdo a donde residen los datos que conlleva al cumplimiento de la normatividad donde estén alojados.
c. Cumpliento con las necesidades de los usuarios en temas de cumplimiento de políticas corporativas, logs, entre otros.
d. Obtener el desempeño deseado, la capacidad es la que se necesita, se tienen bien definidos los ANS (Acuerdos de Nivel de Servicio o SLA en inglés).
e. Razonabilidad sobre cómo opera la seguridad de la información (confidencialidad, integridad y disponibilidad).
f. Confianza sobre manejo de accesos administrativos, un tercero es el que tiene los accesos de alto nivel, cómo tener confianza sobre estos.

En cuanto a la identificación de riesgos, se encuentra información con diferentes enfoques agrupados en seis factores (Gráfica 26), estos permiten de una forma más personalizada evaluar al interior de la organización, se recomienda dar una calificación en cuanto a probabilidad e impacto de cada situación al final se obtendrá una matriz de riesgos sobre la que se podrá trabajar en cómo minimizar su impacto.

Gráfica 26. Factores de riesgo



Fuente: KPMG construcción propia

Funcionalidad

¿Cuál es la posibilidad de que la solución no reúna los requerimientos de negocio, de arquitectura, y de cumplimiento regulatorio? ¿Cómo se impacta la organización?

Confiabilidad

¿Cómo afecta la operación y los resultados la pérdida de calidad de los sistemas/servicios, que en caso de fallas o caídas los planes de recuperación no operen? ¿La seguridad está bien configurada y administrada?

Usabilidad

¿Qué pasa si los servicios/sistemas no operan como fueron planeados? ¿Nuestro personal tienen las capacidades y habilidades para asumir los roles y responsabilidades? ¿Tenemos las personas adecuadas para soportar la solución?

Eficiencia

¿La plataforma contratada si cumple con mis requerimientos de capacidad? ¿Está sobre o sub estimada la capacidad de los recursos? ¿Los ANS se definieron de acuerdo a los criterios de negocio, fueron los sugeridos o son los que generalmente se usan?

Mantenibilidad

¿Conozco mi perfil de riesgo? ¿Los cambios afectan el desempeño de la solución? ¿Qué tan estable es mi solución? ¿Existe un ambiente de pruebas? ¿Realizo los cambios/ajustes en un ambiente de pruebas?

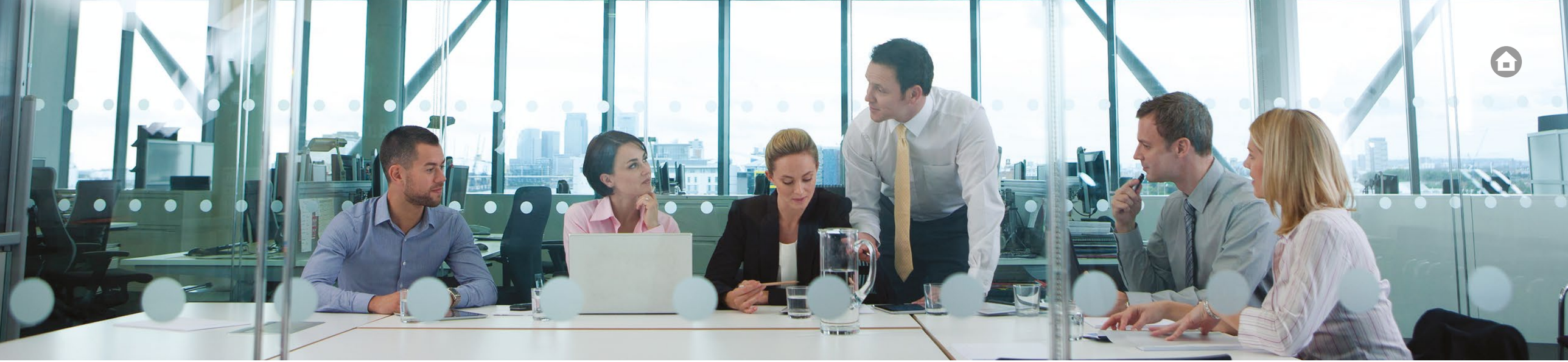
Portabilidad

¿Es fácil cambiarme a otra solución sin que afecte mis datos? ¿Qué tan difícil es evolucionar a nuevas versiones de la solución/servicio?

La administración de riesgos debe ser práctica y fácil de entender, no es necesario enumerar miles y miles de riesgos. Lo importante es que se identifiquen los controles adecuados que los mitiguen; siempre guardando un balance entre el costo y el beneficio de implementar un control.

Otra vista de riesgos a analizar se enfoca en cuatro vértices, ver gráfica 27:

- Financiero
- Regulatorio
- Terceros
- Operación de TI



Gráfica 27. Vértices para el análisis de riesgos

Fuente: KPMG construcción propia

3. Conozca los marcos de control

Conocer los marcos o prácticas de control facilitan la definición de los controles; sin embargo, son teóricos y es necesario apoyarse en tecnologías para hacer el control viable para la organización. Otra premisa a considerar, es que en primera instancia se deben revisar los controles existentes y cómo los mismos pueden soportar la administración de los riesgos identificados.

A continuación se enumeran las organizaciones o instituciones que han trabajado en el tema de cloud y en algún momento puede servir de consulta o soporte (gráfica 28):

Gráfica 28. Principales fuentes de información para cloud computing

Organización	Documento o marco de referencia	Página web
Information System Audit and Control Association (ISACA)	Programas de auditoría	www.isaca.org
Information System Audit and Control Association (ISACA)	Controls and Assurance in the Cloud: using COBITS	http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/controls-and-assurance-in-the-cloud-using-cobit-5.aspx
European Network And Information Segurity Agency (ENISA)	Cloud Computing: benefits, risk and recommendarios for information security	www.enisa.europa.eu
Cloud Security Alliance (CSA)	Top Threats to Cloud Computing V1.0	https://cloudsecurityalliance.org/research/top-threats/
Open Web Application Security Project (OWASP)	10 cloud security risk	https://www.owasp.org/index.php/Main_Page
National Institute of Standards and Tecnology (NIST)	Cloud Computing Synopsis and Recomendations	https://nist.gov/index.html

Fuente: KPMG construcción propia

4. Identifique y pruebe los controles

Los controles deben ser definidos y adaptados a las necesidades de negocio. Adicionalmente, se debe identificar qué riesgo está mitigando, esto con el objetivo de validar el costo beneficio de su implementación, permitiendo a su vez, ver si todos los riesgos están siendo cubiertos y si los controles están mitigando todos los riesgos. En la gráfica 29 se presenta una matriz para el análisis de riesgos y controles.

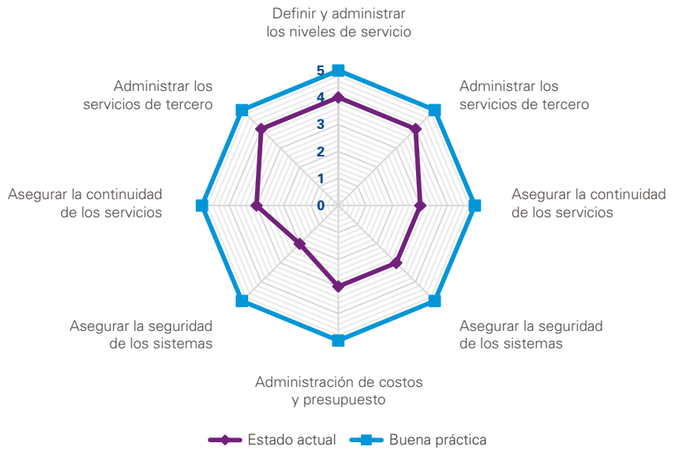
Gráfica 29. Matriz de riesgos vs controles

Riesgos	Controles					
	C1	C2	C3	C4	.....	Cn
R1	x					
R2		x		x		x
R3			x			
:						
Rn	x				x	

Fuente: KPMG construcción propia

En la gráfica 30 se muestran las áreas de control a trabajar cuando tenemos cloud computing. Esta es una propuesta para agrupar los controles y así tener una visión global de los tópicos mínimos a implementar, revisar y probar que estén operando.

Gráfica 30. Áreas de control para cloud computing



Fuente: KPMG construcción propia

5. Realice monitoreo periódico de la efectividad de los controles

Una vez este en operación la nube en su organización y después de tener mapeados riesgos vs controles, no confié ciegamente en sus terceros, evalué por lo menos anualmente como están operando sus controles, no olvide establecer contractualmente las cláusulas que le permitan hacer estas evaluaciones bien sea con sus auditores internos o con profesionales con las competencias adecuadas. Otra opción puede ser exigir contractualmente reportes tipo SAS 70 o sus homólogos.

Las organizaciones más que seguir una tendencia, necesitan optimizar sus costos, una buena forma es utilizar las bondades que ofrece la Nube, sin embargo, evalué temas de gobierno y su alineación estratégica con su negocio, identifique los riesgos propios de su negocio, valide que su personal esté capacitado o busque personal con experiencia y no deje en manos de terceros la toma de decisiones estratégicas. Asegure los temas regulatorios y de impuestos. Finalmente realice las pruebas de los controles periódicamente (por lo menos anualmente).

2.9 Riesgos en blockchain

El rápido crecimiento de esta tecnología emergente ha generado dos grandes retos:

- Lograr entender cómo aplicar, emplear y aprovechar el valor que puede ofrecer blockchain.
- Poder entender y administrar los riesgos asociados.

Una adecuada administración de riesgos permitirá evaluar estas plataformas y a su vez las capacidades tecnológicas para mitigar los posibles impactos negativos para la organización a lo largo del ciclo de vida del producto, desde la selección de la plataforma hasta la prueba de concepto. Las organizaciones deben evaluar las distintas soluciones a lo largo de su ciclo de vida para asegurar que que se adapten a sus necesidades y apetito de riesgo.

Entendiendo los dos tipos de blockchains

- Pública: el acceso está abierto; cualquiera puede convertirse en un nodo y participar en él, Bitcoin es un excelente ejemplo de una cadena de bloques pública.
- Privada: el acceso está limitado a usuarios específicos, como un grupo de bancos, a través de una red privada basada en permisos. Cualquier persona fuera no puede ver ni participar en transacciones.

Tabla 6. Blockchains públicas vs privadas

	Blockchain pública	Blockchain privada
Participación en red	Abierta.	Cerrada.
Privacidad transaccional	No se priorizan, excepto las llamadas monedas.	Ajustable a los deseos de los participantes.
Incentivo económico para la participación	Incorporado.	Organizado por contrato.
Centralización	Totalmente descentralizado.	Grado diverso de descentralización.
Comúnmente utilizado para pagos	Pagos, remesas, mercados de predicción.	Servicio de activos, cambio de divisas (FX).
Redes sociales	Almacenamiento distribuido, redes sociales de pago.	Seguimiento de procedencias, finanzas comerciales, asistencia médica, contratos de seguros.

Aunque cada implementación de Blockchain es única, típicamente incorporarán las siguientes características o alguna combinación de ellas:

- Libro digital inmutable: es el registro no modificable y persistente de la actividad transaccional que utiliza principios criptográficos conocidos, confiables y probados.
- Mecanismo de consenso: mediante el cual los participantes independientes tienen un método acordado sobre cómo se ejecutan las transacciones y cómo se agregan a la cadena de bloques sin depender de intermediarios.
- Identidad y propiedad: si bien la identidad no siempre está vinculada a una identidad del mundo real, generalmente se basa en estos conceptos a través de principios criptográficos para demostrar la capacidad de interactuar y demostrar la propiedad.

Los beneficios claves de la evaluación de riesgos en ambientes blockchain, pueden incluir los siguientes elementos y pueden ser clasificados en una etapa de diseño, desarrollo, despliegue u operación:

- Proveer un modelo holístico para evaluación: un modelo probado para evaluar los riesgos asociados con este tipo de soluciones.
- Apoyar la identificación clara en los riesgos: obtenga información específica en las 10 áreas de riesgo clave asociadas con la implementación de blockchain, incluida la fortaleza de sus controles existentes o propuestos.
- Mover de forma segura las pruebas de concepto a producción: existen riesgos específicos asociados con el paso de las pruebas de concepto a los sistemas de producción. Esto permite tener la identificación de los puntos débiles de su sistema existente antes de que empiece a funcionar.

- Permite la creación de un plan de acción concreto: la evaluación de riesgos proporciona indicadores claros para las áreas críticas de riesgo y las áreas donde se tiene controles menos maduros, para que pueda abordar posibles brechas o debilidades.

Áreas de evaluación de riesgos

Las siguientes son algunas posibles áreas de riesgo que se deben conocer al trabajar este tipo de tecnología:

Mecanismo de consenso y gestión de la red

Se relacionan con la posibilidad de que se registren transacciones inapropiadas, no autorizadas o inexactas. Un mecanismo de consenso, es el medio por el cual los participantes determinan si una transacción es correcta y debería ser aceptada en el blockchain. Si es inefectivo, las transacciones incorrectas podrían ser registradas.

Criptografía, manejo de claves y tokenización

Cada usuario debe mantener un conjunto de claves criptográficas públicas y privadas. Como resultado, es necesario identificar procedimientos para garantizar que estas claves se administran de manera adecuada (por ejemplo, distribución, uso, revocación) para que solo las personas aprobadas accedan a la cadena de bloques. Para mejorar la seguridad, puede ser necesario involucrar a varias personas (dentro de la misma organización participante) antes de completar una transacción. La gestión ineficaz de estas claves podría dar lugar a transacciones o tokens no autorizados.

Gestión de permisos y privacidad

Las blockchain privadas, como se señaló anteriormente:

- Se basan en el principio de que solo los usuarios aprobados pueden unirse y participar en ellas. El uso por partes no autorizadas plantea un riesgo significativo tanto para la integridad y privacidad, como para las transacciones que se registran.
- Requieren la autenticación de las identidades de los participantes, además de políticas y procedimientos de administración de acceso de usuarios a otras aplicaciones confidenciales para permitir solo el acceso de usuarios autorizados.
- Pueden existir diferentes tipos de usuarios a los que solo se les debe permitir realizar ciertas acciones o ver transacciones específicas. Por ejemplo, podría haber un regulador presente en la red. Ese podría tener establecidos sus permisos para que solo pueda ver las transacciones que se encuentran en un estado específico. Por el contrario, un participante comercial solo debe ser capaz de realizar transacciones con partes no reguladoras y no ser capaz de ver o realizar transacciones de las que no es parte.
- Pueden crear inicialmente un entorno menos riesgoso para una solución, pero los riesgos de permisos inapropiados para realizar acciones o permisos de solo lectura en las transacciones pueden tener un impacto significativo en el perfil de riesgo.

Relevancia a los casos de uso y aplicabilidad

Actualmente, hay una cantidad de casos de uso que se están llevando a cabo con respecto a blockchain. Como parte de este proceso, las organizaciones deben considerar, si es relevante usar una u otra solución dadas sus necesidades y objetivos específicos, y si la solución identificada es el método más aplicable y así identificar si es viable poner en producción la solución.

Gestión de datos y segregación

Cualquier empresa involucrada en un blockchain debe evaluar si tiene las capacidades para administrar los casos de uso una vez que se haya creado. Esto incluye la gestión de todos los aspectos de los datos, incluida la confidencialidad, la integridad y la disponibilidad de la información, adicional a la identificación de las fuentes de datos y la comprensión de cómo ocurrirán las actividades cuando los datos no estén disponibles. Así mismo, las organizaciones también deben asegurar que sus actividades cumplan con las regulaciones apropiadas, como las leyes relacionadas a protección de datos personales.

La gestión adecuada de los datos es particularmente crítica cuando dos partes que interactúan en un blockchain desean mantener su transacción anónima de los otros miembros de la red; además de los derechos de uso generales, parte de la información transaccional puede estar en vivo en la blockchain, comúnmente conocida como "en cadena", mientras que otra información puede almacenarse “fuera". Se deben identificar procesos implementados para administrar el movimiento de fondos entre almacenamiento en frío y caliente para que los activos o los fondos no sean transferidos sin los permisos apropiados.

- El almacenamiento en frío: se refiere a soluciones de almacenamiento de claves privadas que están completamente fuera de línea y que generalmente se encuentran en un lugar físicamente seguro. Estas soluciones suelen vivir su ciclo de vida completo sin conectarse nunca a Internet.
- El almacenamiento en caliente: se refiere a los sistemas de almacenamiento de claves privadas que están conectados a Internet y se pueden utilizar para realizar transacciones en tiempo real.

Defensa de la cadena

Las organizaciones que utilizan Blockchain no pueden subestimar los requisitos de seguridad ni hacer suposiciones con respecto a los mecanismos de defensa. Es importante identificar y verificar las pruebas de los procesos de seguridad y monitoreo de la red para reducir los riesgos asociados con cualquier tipo de ataque. Si bien, un proveedor debería realizar el análisis del código fuente como una cuestión de rutina, las organización deben realizar su propia debida diligencia en el código fuente y en cualquier contrato inteligente que se ejecute sobre él, para garantizar que no hayan brechas.

Interoperabilidad e integración

Las organizaciones deben ser conscientes de que sus sistemas heredados pueden no estar diseñados para interactuar con soluciones de blockchain o capitalizar sobre las ventajas que ofrecen. El examen exhaustivo de la interoperabilidad y la integración es esencial para la implementación exitosa. Dada la inmutabilidad de las transacciones, es esencial que existan los mecanismos adecuados para evitar que se ingresen datos incorrectos. Se deben desarrollar controles, tanto de forma independiente como con respecto a las conexiones de protección entre sistemas. A medida que los Blockchain se desarrollan o pasan de prueba de concepto a producción, las compañías también deben garantizar un enfoque adecuado en la gestión de cambios y pruebas, para garantizar que los cambios a escala y alcance no afecten la interoperabilidad y la integración.

Escalabilidad y rendimiento

Los casos de uso proporcionan pruebas de la capacidad para cumplir un propósito específico. Sin embargo, antes de seleccionar una solución o de pasar a un sistema de producción, las organizaciones deben estar seguras de que el blockchain funcionará bajo condiciones lo más parecidas a un ambiente real de producción. Hay muchos factores que pueden influir en la complejidad, y las demandas de cálculo en el nivel de producción que en el caso de uso o incluso en el nivel de prueba de concepto deben considerar (por ejemplo, velocidad y volumen de transacciones, número de participantes activos). Por lo tanto, antes de seleccionar una solución y para su implementación, las organización deben evaluar si la solución es capaz de producir, escalar para crecer y alinearse con su caso de uso.

Continuidad del negocio y recuperación ante desastres.

Al igual que en cualquier otra implementación de tecnología, las organizaciones deben tener un plan para abordar la continuidad

del negocio y los riesgos de recuperación de desastres perteneciente a la aplicación blockchain. La naturaleza descentralizada crea una dependencia única en los otros participantes de la red para mantener la funcionalidad. Dado que las Blockchain privadas pueden tener componentes tanto centralizados como descentralizados (por ejemplo, autoridad de certificación, sistema de gestión de clave de nube), debe haber una comprensión concreta de lo que sucederá si estos componentes se ven afectados por cualquier factor potencial. Esto asegurará que cualquier corte sea limitado y que no se puedan producir transacciones inapropiadas.

Gobierno, riesgo y cumplimiento.

El gobierno general, la gestión de riesgos y el soporte de cumplimiento son esenciales para cualquier implementación. Dado que hay diferentes usuarios - a veces incluso competidores - involucrados, las organizaciones deben ser muy claras en roles específicos y responsabilidades relacionadas con el blockchain. Por ejemplo, cómo las organizaciones gestionarán conjuntamente los cambios de software, incorporación de nuevos nodos u otras actividades. Las funciones y responsabilidades claras y documentadas pueden garantizar que todos los que participan en la cadena de bloques estén en la misma página con respecto a los procesos de cumplimiento.

Convertir la evaluación en acción

Se propone utilizar una escala de madurez de cinco niveles para evaluar la solidez de los controles sobre actividades específicas. Usando esta escala, se puede evaluar los riesgos actuales específicos de Blockchain y definir su estado objetivo para el futuro. Esto permite ayudar a las organizaciones a determinar dónde están más fuertes los controles, dónde existen puntos débiles, vacíos que deben reconocerse y abordarse.

Se debe tener en cuenta que la evaluación de riesgo de esta tecnología no es prescriptiva, sino que se enfoca en identificar áreas clave que requieren mayor atención y acción. Sobre la base de las recomendaciones, los controles reales deben desarrollarse en función de las necesidades únicas de un proyecto o solución blockchain.

El hecho de que una solución esté habilitada con blockchain no significa que aborde los riesgos relevantes, independientemente de lo que puedan pensar algunos proponentes de blockchain. En efecto, blockchain es todavía una tecnología muy joven, con nuevas innovaciones, usos y soluciones que se introducen cada día. Todavía hay muchas lecciones difíciles de aprender de las implementaciones de blockchain, por lo tanto, hacer suposiciones con respecto a los riesgos clave y la seguridad asociados con soluciones específicas podría abrir la puerta a problemas importantes en el futuro.

Para obtener el máximo valor de blockchain, tanto ahora como en el futuro, se debe asumir la responsabilidad de su seguridad; no hay oportunidades o atajos para aprender de los errores de otros. Conduciendo una evaluación de riesgo y luego abordando los riesgos clave asociados con sus actividades especificas, puede asegurarse de que esté bien posicionado para aprovechar las eficiencias y la rentabilidad que proporciona blockchain sin exponerse a riesgos inesperados.

2.10 COBIT 2019 como instrumento para realizar auditoría de tecnología e información

Las organizaciones actualmente se encuentran inmersas en programas de transformación digital soportados en la tecnología y la información para poder lograr el crecimiento rentable y su sostenibilidad en el tiempo. Fundamentalmente, el gobierno empresarial de tecnología e información está relacionado con la entrega de valor desde la transformación digital y la mitigación de los riesgos de negocio resultado de dicha transformación. Por esta razón hemos seleccionado COBIT 2019 como un instrumento para realizar la auditoría de tecnología de información (T&I) debido a que enfoca sus objetivos de gobierno y administración en tres soluciones fundamentales: aportar beneficios, optimizar el riesgo y los Recursos.

La auditoría de tecnología e información debe mostrar el estado actual de los procesos de gobierno y administración de forma independiente y objetiva a través de los mecanismos que ofrece esta última actualización de COBIT. A continuación utilizaremos este marco de referencia para desarrollar todo el ciclo de auditoía de tecnología de información. El ciclo de auditoría que vamos a formular se compone de las siguientes fases planeación, ejecución y reporte.

1. Planeación

Como criterios de selección de los focos de auditoría utilizaremos los cuatro primeros factores de diseño propuestos por COBIT que son estrategia empresarial, metas empresariales, perfil de riesgos y eventos relacionados con tecnología e información.

El primer criterio a considerar es la estrategia empresarial: las organizaciones definen una estrategia principal y COBIT las integra en estas cuatro: crecimiento y adquisición, innovación y diferenciación, administración de los costos, estabilidad y servicio al cliente. Para cada una de estas tácticas COBIT mapea los procesos de su marco de referencia que deben ser objeto de nuestra auditoría. En la tabla 7 podemos observar el mapeo del dominio de evaluar, dirigir y monitorear (EDM) de COBIT 2019 de acuerdo con el planteamiento que tiene la compañía.

Tabla 7. Extracto de mapeo estrategia empresarial con los objetivos de gobierno y gestión de T&I

DF1	Growth/Acquisition	Innovation/ differentiation	Cost leadership	ClientService/stability
EDM01	1,0	1,0	1,5	1,5
EDMO2	1,5	1,0	2,0	3,5
EDM03	1,0	1,0	1,0	**2,0**
EDM04	1,5	1,0	**4,0**	1,0
EDM05	1,5	1,5	1,0	2,0

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

El segundo criterio de selección son las 13 metas de negocio (Enterprise Goals), presentadas en la tabla 8, las cuales están asociadas a una de las cuatro dimensiones del Balanced Scorecard, basados en la metas organizacionales de la organización evaluada, seleccionando cuáles son las metas empresariales más representativas.

Una vez seleccionadas las metas empresariales que están definidas en la organización se identifican las metas de alineación, listadas en la tabla 9, que están asociadas a las metas empresariales, COBIT mapea las metas empresariales con las de alineación indicando cuáles de estas son principales (P) y cuáles son secundarias (S) o cuales no tienen ningún tipo de asociación, permitiendo identificar las metas a las cuales está orienta la tecnología e información en la organización de acuerdo a la tabla 10.

Tabla 8. Metas empresariales COBIT 2019

Referencia	Dimensión BSC	Meta empresarial
EG01	Financiera	Portafolio de productos y servicios competitivos
EG02	Financiera	Gestión de riesgos de negocio
EG03	Financiera	Cumplimiento de regulaciones y leyes externas
EG04	Financiera	Calidad de la información financiera
EG05	Cliente	Cultura de servicio orientada al cliente
EG06	Cliente	Continuidad y disponibilidad del servicio
EG07	Cliente	Calidad de la información gerencial
EG08	Interna	Optimización de los procesos internos de negocio
EG09	Interna	Optimización de costos en los procesos del negocio
EG010	Interna	Competencia, motivación y productividad del personal
EG011	Interna	Cumplimiento de políticas internas
EG012	Aprendizaje y crecimiento	Administración de programa de transformación digital
EG013	Aprendizaje y crecimiento	Innovación de productos de negocio

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Tabla 9. Metas de alineación COBIT 2019

Referencia	Dimensión BSC	Meta empresarial
AG01	Financiera	Cumplimiento y soporte de T&I al cumplimiento del negocio con las leyes y regulaciones externas
AG02	Financiera	Riesgo relacionado con T&I gestionado
AG03	Financiera	Beneficios logrados de las inversiones habilitadas por T&I y el portafolio de servicios
AG04	Financiera	Calidad de la información financiera relacionada con tecnología
AG05	Cliente	Entrega de servicio de T&I en línea con los requerimientos del negocio
AG06	Cliente	Agilidad para convertir los requerimientos del negocio en soluciones operativas
AG07	Cliente	Seguridad de información, infraestructura de procesamiento, aplicaciones y privacidad
AG08	Interna	Habilitar y soportar los procesos del negocio mediante la integración de aplicaciones y tecnología
AG09	Interna	Entrega de programas en tiempo, presupuesto y logrando los requerimientos y estándares de calidad
AG010	Interna	Calidad de la información de la gerencia de T&I
AG011	Interna	Cumplimiento de T&I con las políticas internas
AG012	Aprendizaje y crecimiento	Personal competente y motivado con el entendimiento mutuo del negocio y la tecnología
AG013	Aprendizaje y crecimiento	Conocimiento, experiencia e iniciativas para la innovación del negocio

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Por ejemplo, seleccionamos la meta empresarial EG09 - Optimización de costos en los procesos del negocio, al revisar el mapa de alineación propuesto por COBIT observamos que este objetivo empresarial tiene como meta de alineación principal la AG04 - Calidad de la información financiera relacionada con tecnología y como metas de alineación secundaria la AG03 - Beneficios logrados de las inversiones habilitadas por T&I y el portafolio de servicios, AG09 - Entrega de programas en tiempo, presupuesto y logrando los requerimientos y estándares de calidad y AG10 - Calidad de la información de la gerencia de T&I. Estas metas de alineación son las asociadas a la Tecnología e Información que apalancan el cumplimiento de la meta empresarial y que serán objeto de la auditoría.

Tabla 10. Mapa de alineación.

	EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	E013
AGO1		S	P								S		
AGO2		P				S							
AGO3	S				S			S	S			P	
AGO4				p			p		p				
AGOS	P				S	S		S				S	
AGOG	P				S			S				S	S
AGO7		P				P							
AGO8	P				P			S		S		P	S
AG®	P				S			S	S			P	S
AG10				p			p		S				
AG11		S	P								P		
AG12					S					P			
AG13	P		S									S	P

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Una vez identificadas las metas empresariales en las que está enfocada la organización auditada, permite determinar los procesos de Tecnología e Información de COBIT 2019 que están apalancando el cumplimiento de esta meta y que serán incluidos en el plan de auditoría como objetivo de gobierno y administración a evaluar. En la tabla 11 se evidencia el mapeo de las metas y los procesos del dominio EDM de Tecnología e Información propuestos por COBIT.

Continuando con el ejemplo al seleccionar la meta de alineación principal la AG04 - Calidad de la información financiera relacionada con tecnología de acuerdo con la tabla 9 el proceso objeto de auditoría para cubrir esta meta sería el APO06 - administración de costos y presupuesto considerando únicamente este criterio, porque al ponderar los otros tres criterios tendremos una vista consolidada de los procesos a auditar.

El tercer criterio que vamos a considerar es el perfil de riesgo de tecnología e información de la organización, COBIT propone 19 escenarios de riesgos de tecnología, listados en la tabla 12, a los que actualmente se encuentra expuestas las organizaciones y que deben ser evaluados para determinar los procesos que están enfocados a la mitigación de esos riesgos. Es de aclarar que se puede realizar un mapeo más extenso de riesgos adicionales que la organización haya identificado, pero COBIT propone 19 riesgos principales.

Tabla 11. Extracto de mapeo metas alineadas con los objetivos de gobierno y gestión de T&I

	AGO1	AGO2	AGO3	AGO4	AGO5	AGO6	AGO7	AGO8	AGO9	AGO10	AGO11	AGO12	AGO13
EDM01	P	S	P					S			S		
EDMO2			P		S	S		S					S
EDM03	S	P					P				S		
EDM04			S		S	S		S	P			S	
EDM05				S						P	S		

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Tabla 12. Categoría de riesgos de T&I COBIT 2019

Referencia	Categorías de riesgos de T&I
RISKCAT01	Toma de decisiones de inversiones de TI y mantenimiento y definición del portafolio
RISKCAT02	Administración del ciclo de vida de programas y proyectos
RISKCAT03	Sobrecostos de TI
RISKCAT04	Experiencia, habilidades y comportamiento del Staff de T&I
RISKCAT05	Arquitectura empresarial de T&I
RISKCAT06	Incidentes en la infraestructura operacional de TI
RISKCAT07	Acciones no autorizadas
RISKCAT08	Problemas en la adopción y uso del software
RISKCAT09	Incidentes de hardware
RISKCAT10	Fallas en el software
RISKCAT11	Ataques lógicos (hacking, malware, etc.)
RISKCAT12	Incidentes con terceros o proveedores
RISKCAT13	No cumplimiento
RISKCAT14	Eventos geopolíticos
RISKCAT15	Acciones industriales
RISKCAT16	Actos de la naturaleza
RISKCAT17	Innovación basada en tecnología
RISKCAT18	Medio ambiente
RISKCAT19	Administración de datos e información

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Al seleccionar las categorías de riesgos a los que está expuesta la organización auditada se identifican los procesos de COBIT que deben ser evaluados porque necesitan una adecuada gestión para la mitigación de dichos riesgos en la organización. COBIT realiza el mapeo y sugiere unos procesos de acuerdo a la tabla 13 en donde se muestra la relación con los procesos del Dominio EDM.

El cuarto criterio a considerar en la planeación de la auditoría son los eventos materializados relacionados con tecnología e información, COBIT los agrupa en los siguientes 20 eventos de la tabla 14, los cuales deben ser analizados para seleccionar aquellos que se hayan presentados en el periodo de análisis, típicamente, en el último año para sí poder mapear los procesos asociados a dichos eventos de riesgo materializados.

Tabla 13. Extracto de mapeo metas alineadas con los objetivos de gobierno y gestión de T&I

DF3	RISKCATO1 IT Investment Decision Making, Portfolio Definition & Maintenance	RISKCATO2 Program & Projects Life Cycle Management	RISKCATO3 IT Cost & Oversight	RISKCATO4 IT Expertise, Skills & Behavior	RISKCATO5 Enterprise/ IT Architecture	RISKCATO6 IT Operational Infrastructure Incidents	RISKCATO7 Unauthorized Actions	RISKCATOB "Software Adoption/ Usage Problems"	RISKCATO9 Hardware Incidents	RISKCAT1 0 Software Failures
EDM01	3	2	3	0	0	0	2	0	0	0
EDMO2	3	2	0	0	2	0	0	0	0	0
EDOM3	2	2	0	0	0	0	0	0	0	1
EDM04	3	0	4	3	2	0	0	0	0	0
EDM05	3	1	3	0	0	0	2	0	0	1

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Tabla 14. Categoría de eventos de riesgos de T&I COBIT 2019

Referencia	Categorías de riesgos de T&I
A	Frustración entre las diferentes entidades de TI en toda la organización debido a la percepción de una baja contribución de valor al negocio.
B	Frustración en las áreas de negocio (es decir el cliente de TI) y el departamento de TI por errores en las iniciativas o percepción de una baja contribución al valor empresarial.
C	Incidentes significativos relacionados con TI, como pérdida de datos, violaciones de seguridad, fallas en proyectos, errores de aplicaciones, etc.
D	Problemas en la entrega del servicio por parte de los proveedores de TI.
E	Incumplimiento de los requisitos reglamentarios o contractuales relacionados con TI.

Referencia	Categorías de riesgos de T&I
F	Resultados de auditorías periódicas u otros informes de evaluación sobre el bajo rendimiento de TI o baja calidad del servicio de TI .
G	Costos ocultos sustanciales no autorizados, es decir, gastos en TI por parte de los usuarios fuera del control de los mecanismos normales de decisión de inversión en TI y presupuestos aprobados.
H	Duplicaciones entre varias iniciativas u otras formas de desperdicio de recursos.
I	Recursos de TI insuficientes, personal con habilidades inadecuadas o insatisfacción del personal.
J	Cambios o proyectos de TI que con frecuencia no satisfacen las necesidades del negocio y se entregan tarde o sobrepasan el presupuesto.
K	Renuencia por parte de los miembros de la Junta, los Ejecutivos o la Alta Gerencia para interactuar con TI, o la falta de compromiso de los patrocinadores de negocios para TI.
L	Modelo operativo complejo de TI y / o mecanismos de decisión poco claros para decisiones relacionadas con TI.
M	Costo excesivamente alto de TI.
N	Implementaciones fallidas de nuevas iniciativas o innovaciones causadas por la arquitectura de TI y los sistemas actuales.
O	Brecha entre el conocimiento técnico y del negocio que lleva a los usuarios y a TI y / o especialistas de tecnología que hablan diferentes idiomas.
P	Problemas regulares con la calidad de los datos y la integración de los datos provenientes de varias fuentes.
Q	Alto nivel de cómputo del usuario final, lo que crea (entre otros problemas) una falta de supervisión y control de calidad sobre las aplicaciones que se están desarrollando y poniendo en funcionamiento.
R	Las áreas del negocio implementan sus propias soluciones de información con poca o ninguna participación del departamento de informática.
S	Ignorancia y / o incumplimiento de las normas de seguridad y privacidad.
T	Incapacidad para explotar nuevas tecnologías o innovar usando I&T.

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Los eventos de riesgos seleccionados por el auditor que está realizando la planeación permitirán elegir los procesos a auditar basado en el mapeo de los eventos con los procesos de COBIT presentados en la tabla 14.

Al concluir el análisis de estos cuatro criterios se obtienen los procesos de COBIT que deben ser seleccionados para la planeación de la auditoría, teniendo en cuenta esto se sugiere realizar una matriz donde se incluyan los cuatro criterios con la ponderación sugerida en la guía de diseño de COBIT 2019, extraer las tablas completas de la guía de diseño de COBIT 2019 para de forma objetiva seleccionar los procesos a auditar y así concluir la planeación de la auditoría.

2. Ejecución

Luego de seleccionar los procesos objeto de la auditoría en la planeación se utiliza el marco de referencia de COBIT denominado "Objetivos de Gobierno y Gestión" en donde por cada uno de los procesos identificamos las prácticas de administración y las actividades que se deben realizar para dar cumplimiento al objetivo propuesto.

COBIT describe detalladamente las prácticas de administración y las actividades que permitirán al auditor entender cómo estás están siendo aplicadas en la organización y formular el plan de pruebas a ejecutar para realizar la prueba de diseño y de eficacia operativa que permitan concluir que la actividad se está ejecutando al interior de la organización.

Para la medición de estos procesos también se tienen en cuenta los siete componentes propuestos por COBIT y que podrían considerarse en cada proceso evaluado:

1. Procesos
2. Estructuras organizacionales
3. Flujos de información e ítems
4. Personas, habilidades y competencias
5. Políticas y procedimientos
6. Cultura, ética y comportamiento
7. Servicios, infraestructura y aplicaciones

COBIT en su versión 2019 por cada proceso ha incluido una relación de guía a buenas prácticas adicionales que nos pueden servir como marcos de referencia para profundizar en las actividades de control que deben ser ejecutadas para mejorar el sistema de control interno y que se pueda emplear en la definición del plan de pruebas.

3. Reporte

Para la generación del reporte COBIT 2019 propone el uso de un proceso de evaluación de niveles de capacidad el cual está basado en el esquema de capacidad propuesto por CMMI que va desde el nivel 0 al nivel 5, donde el 0 es inexistente y el 5 está en capacidad de mejora continua como se muestra en la tabla 15.

Para realizar una evaluación objetiva COBIT propone que para estar en un nivel de capacidad específico se debe probar que todas las actividades de ese nivel se realicen de forma consistente para así poder concluir el nivel de capacidad del proceso.

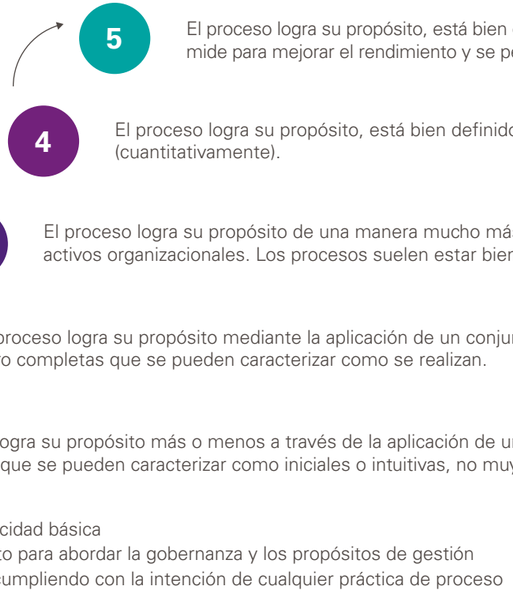
En la generación del reporte de auditoría de cada proceso se propone incluir el nivel de capacidad propuesto por COBIT 2019 incluyendo recomendaciones para el cierre de brechas identificadas basadas en las buenas prácticas de este marco de referencia y los relacionados como sugerencia en cada uno de los procesos.

Tabla 15. Extracto de mapeo metas alineadas con los objetivos de gobierno y gestión de T&I

DF4	Frustration between different IT entities across the organization because of a perception of low contribution to business value	Frustration between business departments (i.e., the IT customer) and the IT department because of failed initiatives or a perception of low contribution to business value	Significant IT related incidents, such as data loss, security breaches, project failure and application errors, linked to IT	Service delivery problems by the IT outsourcer(s)	Failures to meet IT-related regulatory or contractual requirements	Regular audit findings or other assessment reports about poor IT performance or reported IT quality or service problems
EDM01	[1] 3,0	3,0	1,0	1,0	2,0	2,0
EDMO2	2.5	3,0	1,0	1,0	1,5	2,5
EDOM3	1,0	1,0	2,0	1,0	2,0	2,0
EDM04	1,0	1,0	1,0	1,0	1,0	2,0
EDM05	1,0	1,0	1,0	1,0	1,5	2,0

Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Gráfica 31. Niveles de capacidad



Fuente: COBIT 2019 Designing an Information and Technology Governance Solution

Referencias

- Marsh Risk Consulting; RIMS. (Enero de 2018). Tomado de Marsh LLC: https://www.marsh.com/co/insights/research/iii-benchmark-de-gestion-de-riesgos-en-latinoamerica.html
- Chambers, R. F. (Agosto de 2018). The Institute of Internal Auditors. Obtenido de Auditoría interna y Riesgos Emergentes: desde la cima de la colina al escritorio: https://global.theiia.org/knowledge/chambers-spanish/Pages/Auditoria-interna-y-Riesgos-Emergentes-desde-la-cima-de-la-colina-al-escritorio.aspx
- Auditoría, I. d. (26 de Abril de 2017). El rol actual de la Auditoría Interna. Obtenido de https://iaia.org.ar/rol-actual-la-auditoría-interna/
- BBVA. (s.f.). Obtenido de https://www.bbva.es/general/finanzas-vistazo/empresas/joint-venture/index.jsp
- KPMG Internal Audit: Top 10 in 2019 Considerations for impactful internal audit departments. Number 7: Culture Risk
- https://home.kpmg/co/es/home/media/Notas%20de%20prensa/2017/02/la-gestion-de-riesgos-es-lo-que-mas-preocupa-a-los-comites-de-auditoria.print.html
- https://intra.ema.kpmg.com/sites/GQRM/
- Norma Técnica NTC-ISO 31000 del 18 de julio de 2018
- Ministerio de Salud y Protección Social. (2018). Lineamiento técnico y operativo de la Ruta Integral de Atención para Promoción y Mantenimiento de la salud. Recuperado el 16 de Octubre de 2018, de https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/VS/PP/lineamiento-ruta-promocion-mantenimiento.pdf
- Villar Aguirre, Manuel. (2011). Factores determinantes de la salud: Importancia de la prevención. Acta Médica Peruana, 28(4), 237-241. Recuperado en 25 de octubre de 2018, de
- http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1728-59172011000400011&lng=es&tlng=es.
- Organización Mundial de la Salud. (2018). Comunicado de prensa. Recuperado el 27 de octubre de 2018, de http://www.who.int/es/news-room/detail/02-05-2018-9-out-of-10-people-worldwide-breathe-polluted-air-but-more-countries-are-taking-action
- Jiménez, P., & Nereida, D. (2011). La gestión del riesgo en salud en Colombia (Doctoral dissertation, Universidad Nacional de Colombia).
- Federación de Aseguradores Colombianos-FASECOLDA. (2018). Sistema de Administración de Riesgo. Recuperado el 18 de Octubre de 2018, de http://www.fasecolda.com/index.php/fasecolda/asuntos-financieros/sistema-de-administracion-de-riesgos/
- Zenklussen, M. B. Modelo de gestión de riesgo-Enterprise Risk Management (ERM)-Análisis en empresa local de Rafaela: Elsener Pinturas SA. Recuperado el 28 de Octubre de 2018, de http://pa.bibdigital.uccor.edu.ar/1390/2/Modelo%20de%20Gesti%C3%B3n%20de%20riesgo.%20ERM.%20ELSENER%20PINTURAS%20S.A.DIC%202016.Para%20Imprimir.VF.pdf
- Decreto 726 de 2018 del Ministerio del Trabajo. Artículo 1. Modificación del Capítulo 2 del Título 9 de la Parte 2 del Libro 2 del Decreto 1833 de 2016. Modifíquese el Capítulo 2 del Título 9 de la Parte 2 del Libro del Decreto 1833 de 2016 que compila las normas del Sistema General de Pensiones
- Cyxtera, (2018). The Fraud Bet. Recuperado el 27 de abril de 2019, de https://www.easysol.net/images/stories/downloads/es-fraudbeat2018.pdf
- Centro Cibernético Policial. (2015). Boletín de Análisis Estratégico en CIBERSEGURIDAD. Recuperado el 27 de abril de 2019, de https://caivirtual.policia.gov.co/sites/default/files/bacib_001_6_0.pdf
- Harvey Nash, KPMG. (2018). CIO Survey 2018. Recuperado el 28 de abril de 2019, de https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/06/harvey-nash-kpmg-cio-survey-2018.pdf
- IBM Security, Ponemon Institute LLC. (2018). 2018 Cost of a Data Breach Study: Global Overview. Recuperado el 28 de abril de 2019, de https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf
- KPMG LLP, (2019). The role of internal audit in cyber security readiness.
- Security Exchange Commission. (2018). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements. Release No. 84429. Recuperado el 28 de abril de 2019, de www. sec.gov https://www.sec.gov/litigation/investreport/34-84429.pdf
- Security Exchange Commission. (2018). SEC Office of Compliance Inspections and Examinations Announces 2019 Examination Priorities. Recuperado el 28 de abril de 2019, de www.sec.gov https://www.sec.gov/news/press-release/2018-299
- Teniente Coronel Durán, A. U. (2019). Contexto del Cibercrimen en Colombia. Recuperado el 28 de abril de 2019, de https://www.ccce.org.co/sites/default/files/biblioteca/policia-nacional-ciberseguridad.pdf
- Cloud Security Alliance, 'Top Threats to Cloud Computing V1.0', March 2010, www.cloudsecurityalliance.org/topthreats
- ENISA, 'Cloud Computing: Benefits, Risks and Recommendations for Information Security', 2009, www.enisa.europa.eu
- Halpert Ben, Auditing cloud Computing: a security and privacy guide, John & Sons, Inc, 2011
- IT trends for 2013, http://blogs.sap.com/innovation/innovation/it-trends-for-2013-023913
- ISACA, Cloud Governance, 2013
- KPMG INTERNATIONAL, Breaking Through the cloud adoption Barriers, 2013 kpmg.com/cloud
- Kelson Norm, Cloud Computing Mangement Audit/Assurance Program, ISACA, 2010
- Lo Shandy, IT trends for 2013, SAP BLOG, 2012, http://blogs.sap.com/innovation/innovation/it-trends-for-2013-023913
- Prince Brian,Identifiying and Remediating Security Vulnerabilties in the Cloud, Information Week Reports, 2013
- Rhoton John, Cloud Computing Protected, Recursive Limited, 2013
- Vohradsky David, Cloud Risk- 10 Principle and a Framework for Assesment, Journal Volumen 5 ISACA, 2012
- COBIT 2019, 'Framework Governance and Management Objectives', 2018. ISACA
- COBIT 2019, 'Introduction and Methodology', 2018. ISACA
- COBIT 2019, 'Designing an Information and Technology Governance Solution', 2018. ISACA
- COBIT 2019, 'Implementing and Optimizing an Information and Technology Governance Solution', 2018. ISACA

Glosario

AEGR	Auditoría Externa de Gestión y Resultados
AFP	Administradora de Fondos y Pensiones
AI	Auditoría Interna
ANS	Acuerdos de Niveles de Servicio
CCU	Condiciones Uniformes de los Contratos
D&A	Data & Analytics
DANE	Departamento Administrativo Nacional de Estadística
DEA	Director Ejecutivo
EAPB	Entidades Administradoras de Planes de Beneficios en Salud
ERM	Gestión de Riesgos Empresariales
GDPR	General Data Protection Regulation
GIRS	Gestión Integral de Riesgos en Salud
GRC	Gobierno, Riesgo y Cumplimiento
IaaS,	Infraestructura como un Servicio
IBRL	Ingreso Base de Liquidación
IARCS	Servicios de Cumplimiento, Riesgo y Auditoría Interna
IIA	Instituto de Auditores Internos
IPS	Instituciones Prestadoras de Servicios
ISS	Instituto de Seguridad Social
KPIs	Indicadores Claves de desempeño
MIAS	Modelo de Atención Integral en Salud
MSPS	Ministerio de Salud y Protección Social
NTC	Norma Técnica Colombiana
NYDFS	New York Department of Financial Services
OCTE	Office of Compliance Inspections and Examinations
PaaS	Plataforma como un servicio
PAIS	Politica de Atención Integral en Salud
PDSP	Plan Decenal de Salud Pública
QA	Evaluación de Calidad
RAIS	Régimen de Ahorro Individual con Solidaridad
RIAS	Rutas Integrales de Atención en Salud
RMP	Régimen Solidario de Prima Media con Prestación Definida
RUPS	Registro Único de Prestador del Servicio
SaaS	Software como un Servicio
SAR	Sistema de Administración de Riesgos
SARL	Sistema de Administración de Riesgo de Liquidez
SARM	Sistema de Administración de Riesgo de Mercado
SEC	"Securities and Exchange Commission" Agencia federal encargada de la supervisión de los mercados financieros
SMMLV	Salario Mínimo Mensual Vigente
SSPD	Superintendencia de Servicio Públicos Domiciliario
SUI	Sistema único de Información
UGPP	Unidad de Gestión Pensional y Parafiscal
SPA	Sustancias Psicoactivas


KPMG