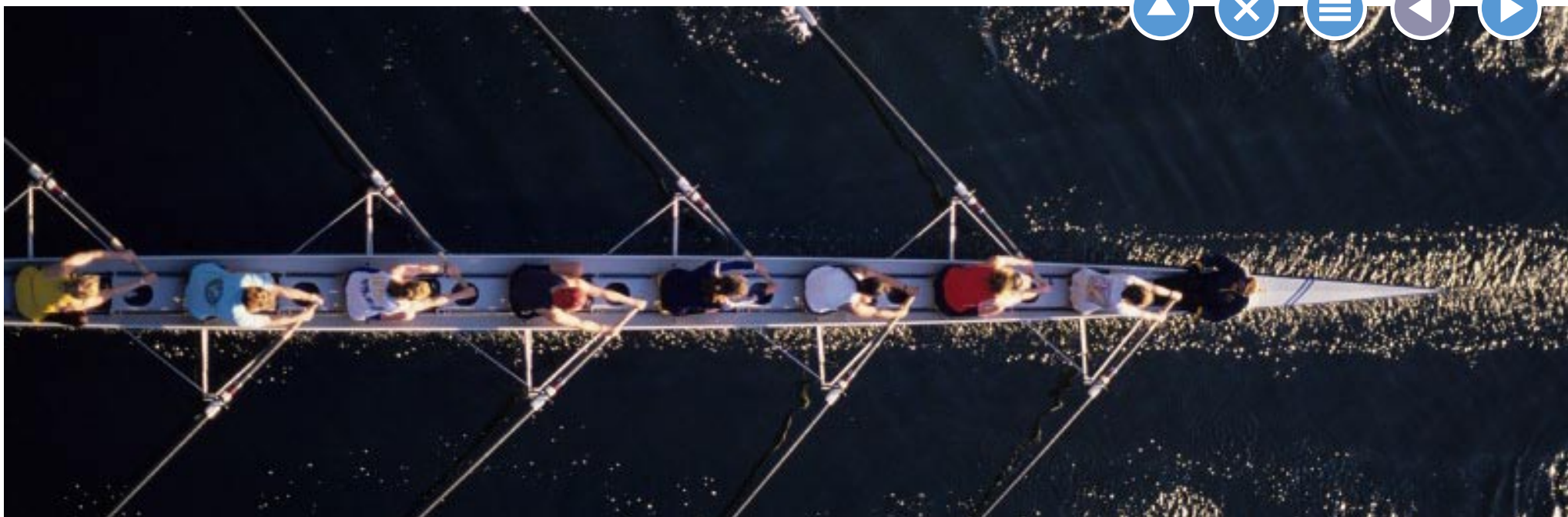


Boletín de Asesoría Gerencial*

Cómo alcanzar la gobernabilidad en las organizaciones

No. 14 - 2008

Contenido Cerrar Imprimir Página anterior Página siguiente



ESPIÑEIRA, SHELDON Y ASOCIADOS

Firma miembro de

PRICEWATERHOUSECOOPERS 

Contenido

Haga click en los enlaces para navegar a través del documento



Haga click en los enlaces para llegar directamente a cada sección

- ▶ Introducción
- ▶ Años 60's
- ▶ Años 70's
- ▶ Años 80's
- ▶ ¿Qué ha pasado desde los años 90's?
- ▶ Las organizaciones del presente y futuro. ¿Qué está pasando actualmente?
- ▶ Necesidad de organizar la Gestión Integral de Riesgo
- ▶ Gobernabilidad en las organizaciones
- ▶ Roles y responsabilidades
- ▶ Conclusión
- ▶ Créditos / Suscribirse

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones



Introducción

Las grandes pérdidas financieras que han impactado el patrimonio y reputación de algunas organizaciones, la sofisticación en el mundo de los negocios, la globalización, la alta competencia, la operativa diaria de las diferentes industrias y el desarrollo de la tecnología, han impulsado acciones por parte de los empresarios y organismos regulatorios en función de alcanzar un consenso que sea capaz de alinear los diversos intereses involucrados para maximizar los beneficios y ser más eficientes en el cumplimiento y en la oferta a los clientes.

El reto presente es la alineación de las actividades de las diversas unidades de negocio operativas y de control, tales como: tecnología de información, seguridad de información, gestión integral de riesgo, auditoría y contraloría. Ahora bien: ¿qué ha sucedido en los últimos años para que el concepto de gobernabilidad haya cobrado interés?.

A continuación se presenta una reseña histórica de la evolución de las unidades tanto operativas como de control, así como también se resalta la importancia de la Gobernabilidad en las organizaciones, para finalmente listar los roles y responsabilidades de estas unidades, enmarcadas, según nuestra experiencia, en el contexto local venezolano con algunas referencias internacionales.

Años 60's

Tecnología y Seguridad de la Información:

A principios de los años 60's comienza el uso de Mainframes diseñados para procesar enormes cantidades de información en poco tiempo. Surge la ejecución de procesos por lotes (batch), con el uso de una computadora secundaria encargada de realizar las operaciones de entrada y salida, donde eran colocados los lotes de trabajo que se procesarían en el computador principal (único encargado del procesamiento), el cual procesaba los datos y enviaba los resultados a la computadora secundaria para que ésta realizara las operaciones de salida.

Bajo este esquema, existía una excesiva centralización del procesamiento de información con múltiples interfaces de aplicaciones y era utilizada una tecnología costosa y poco flexible.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Años 60's (continuación)

Pocos procesos básicos de negocio eran apoyados por la Función de Tecnología de Información ya que el enfoque se encontraba orientado principalmente a la gestión de la infraestructura tecnológica. La Función de Tecnología de Información era comúnmente un departamento dentro de la Gerencia de Administración y Finanzas, tal como se muestra en la Figura N° 1.

Al final de la década de los 60's, surgen las primeras iniciativas de seguridad de información, impulsadas en sus inicios por el Departamento de Defensa de los Estados Unidos después de la implantación de la ARPANet en 1969. En esta década, los riesgos principales incluían la búsqueda de claves secretas, hurto de tarjetas de crédito en correspondencias, y uso de la técnica salami (tipo de fraude cuyo nombre se debe a que el delito de comete por pequeñas tajadas o

cortes). Los riesgos asociados a la seguridad de la información, eran vistos como aspectos netamente técnicos, y la conciencia en seguridad de información, era inexistente o imperceptible.

Para ampliar: haga click sobre la imagen

[Retorno](#)

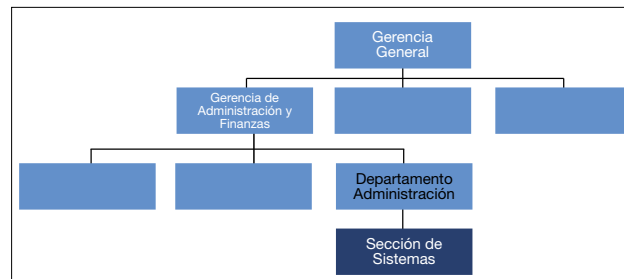


Figura N° 1. Estructura de las organizaciones en los años 60's

Contraloría, Auditoría y Riesgo:

Las unidades de control tenían funciones básicas. En el área contable, los departamentos estaban estructurados con gran cantidad de personas, dedicadas al registro y contabilización de todas las transacciones que se efectuaban.

Normalmente, el personal dentro de los departamentos de contabilidad se dividía por áreas de los estados financieros, y en ocasiones se les llamaba “custodios de cuenta”. Era imprescindible que concentraran toda la documentación que se manejaba, porque con ella se preparaban los asientos contables.

El desarrollo de la tecnología para los sistemas contables era muy básico, por lo que la intervención del personal para la contabilización de operaciones era muy alta.

Las actividades de control de las operaciones se centraban en la revisión de la integridad de los balances y eran realizadas por las personas de mayor nivel jerárquico de los departamentos. En cuanto a las áreas de auditoría, estas se enfocaban en la revisión de la veracidad de la documentación que respaldaba los pagos y asientos contables, a los arqueos de caja chica para revisar los manejos del efectivo, inventarios de materiales y equipos, con el fin de revisar su existencia física, entre otros.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Años 70's

Tecnología y Seguridad de la Información:

En esta época se inicia el uso de las microcomputadoras y los sistemas en línea. Comienza a utilizarse los puntos de ventas (POS) y Automatic Teller Machine (ATM) y son definidas las redes privadas y las transacciones de transferencia electrónica de fondos.

Asimismo, surgen los primeros esfuerzos para la definición de la seguridad de información, definiendo modelos teóricos, como Bell-LaPadula (1973) y Biba (1975) donde se establecieron algunos de los primeros conceptos de confidencialidad e integridad de la información, enfocados a la mitigación de los riesgos presentes tales como: fraude en el arqueo y manipulación de los ATM's, retención de las tarjetas de crédito y débito en los ATM's y falsificación de plásticos.

Los administradores de bases de datos tenían la responsabilidad de la seguridad de la información, iniciándose la implantación de filtrado de tráfico de red en dispositivos como routers. En Venezuela, un banco desarrolla el primer manual de políticas de seguridad de la información.

Con respecto a la década anterior, la Función de Tecnología es ampliada hacia la programación y estructuración de los datos, incorporando ciertos elementos de control como producto de las innovaciones tecnológicas; sin embargo, esta unidad continúa reportando a la Gerencia de Administración y Finanzas, tal como se muestra en la Figura N° 2.

Contraloría, Auditoría y Riesgo:

En cuanto a las unidades de control, tenemos que las funciones contables eran ejecutadas por un Departamento de Contabilidad, cuyos integrantes debían poseer estos conocimientos para ejercer su labor. El desarrollo de la tecnología y la

Para ampliar: haga click sobre la imagen

[Retorno](#)

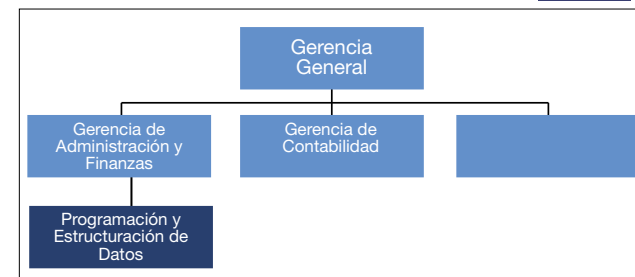


Figura N° 2. Estructura de las organizaciones en los años 70's

aparición del concepto de base de datos relacional, permitieron la evolución de los sistemas contables que, si bien es cierto que las principales transacciones contables eran registradas por las computadoras, la función del Departamento, era revisar estas transacciones e incorporar los asientos contables que no estaban automatizados. En la mayoría de las ocasiones, la toma de decisiones y el control de operaciones, no era oportuno.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones



Años 70's (continuación)

Normalmente, se requería una gran cantidad de personas para mantener la contabilidad actualizada. De hecho, las organizaciones podían tener acceso a los estados financieros entre veinte (20) y treinta (30) días después del cierre contable de cada mes.

Los auditores internos empiezan a especializarse en el análisis de los sistemas contables para obtener evidencia del funcionamiento de la tecnología, en cuanto al registro de las transacciones.

A nivel internacional y para el sector financiero, en 1974 fue establecido el Comité de Basilea, como el Comité de Regulación Bancaria y Prácticas Supervisoras, por los bancos centrales del Grupo de los Diez (G-10), como resultado de la turbulencia monetaria y bancaria internacional.

Años 80's

Tecnología y Seguridad de la Información: Continúa el desarrollo de los marcos teóricos de seguridad: en 1985 se establece el primer criterio de seguridad para sistemas en el "Trusted Computer System Evaluation Criteria" conocido también como libro naranja del Departamento de Defensa de los Estados Unidos, donde se establecen clasificaciones de seguridad para los sistemas con base en su modelo de control de acceso y características de seguridad.

Adicionalmente, en 1987 se publica el modelo Clark-Wilson, donde se establece por primera vez el concepto de "segregación de funciones". En agosto de 1981 IBM lanza al mercado su primera computadora personal, llamada IBM PC.

En estos años, surgen las primeras versiones de servicios electrónicos, portales Web, y servicio IVR. Ocurren los primeros intercambios de información

electrónica entre las organizaciones, mediante enlaces dedicados como EDI (Electronic Data Interchange) y SWIFT (Society for Worldwide Interbank Financial Telecommunication). Ocurre un cambio de la orientación basada en la gestión y administración de la infraestructura tecnológica, orientándose a la gestión del apoyo de la tecnología a los procesos y funciones de negocio apoyados por el surgimiento de los primeros sistemas ERP (Enterprise Resource Planning).

Los riesgos presentes para esta época, afectaban principalmente en la legitimación de capitales, captura de datos en las redes y clonación de tarjetas de débito y crédito, incrementándose notablemente los fraudes en los POS. En esta década, los riesgos asociados a la tecnología eran vistos como simples intentos de violar la protección de los sistemas o del perímetro, por lo tanto se le presta poca importancia y se deja la seguridad en manos de los administradores de red, que entienden de los elementos más técnicos.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Años 80's (continuación)

Con respecto a la estructura organizativa, se inicia la separación entre las funciones de la Gerencia de Administración y Finanzas y la Gerencia de Programación y Estructuración de Datos, formalizándose las actividades relacionadas con la administración de seguridad de la información (ver Figura N° 3).

Para ampliar: haga click sobre la imagen

 Retorno

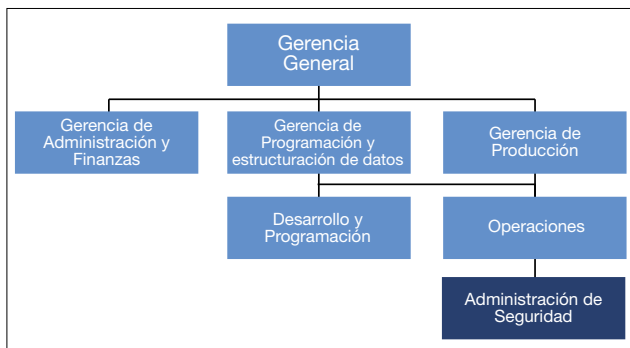


Figura N° 3. Estructura de las organizaciones en los años 80's

Contraloría, Auditoría y Riesgo:

En cuanto a los aspectos de control y con el avance de la tecnología, se producen cambios en la forma de auditar ya que se incorporan técnicas de revisión sobre la base de sistemas computarizados. Para los departamentos de contabilidad, se desarrollaron sistemas que cada vez más facilitaban las labores de registro contable.

Es por ello que comienza a aparecer la figura de Gerencia de Contabilidad, donde la revisión de los asuntos contables y la creación de reportes, se convierte en las principales labores de esta gerencia, cuya línea de reporte seguía estando adscrita a la ya conocida Gerencia de Administración y Finanzas.

Por otro lado, en 1985 se forma la Comisión Nacional para Emisión de Informes Fraudulentos, conocida como la Treadway Commission, a fin de identificar las causas en la proliferación de emisión de informes fraudulentos; y en 1987 esta

comisión solicita realizar un estudio para desarrollar una definición común del control interno y marco conceptual. Finalmente en 1988, el Comité de Organizaciones Patrocinantes de la Comisión Treadway, conocido como COSO, seleccionó a Coopers & Lybrand para estudiar el control interno.

A nivel internacional y para el sector financiero, a principios de los años 80, los coeficientes de capital de los principales bancos internacionales estaban deteriorándose y, al mismo tiempo, los riesgos asumidos aumentaban. Respaldado por el G-10, el Comité de Basilea decidió trabajar en una medida de adecuación de capital hacia la cual convergieran los países miembros, y en julio de 1988, fue aprobado por el G-10 un sistema de medición del capital, conocido como el Acuerdo de Basilea. Dicho sistema, contemplaba un requerimiento mínimo de capital, así como principios básicos de supervisión para el sector financiero.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Años 80's (continuación)

Desde entonces, el Acuerdo ha sido adoptado no sólo en países miembros del G-10 sino en prácticamente todos los países con bancos internacionalmente activos.

¿Qué ha pasado desde los años 90's?

Tecnología y Seguridad de la Información: Los años 90's inician con una nueva estructura organizacional propuesta para la Función de Seguridad de la Información (ver Figura N° 4), en donde ésta unidad se conforma como un área especializada dentro de la Función de Tecnología de Información y posee personal y recursos propios.

Para ampliar: haga click sobre la imagen

[Retorno](#)

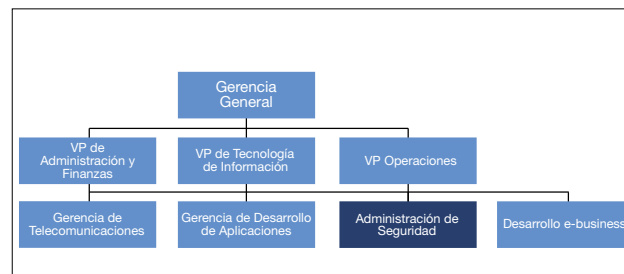


Figura N° 4. Estructura de las organizaciones a principios de los años 90's

Empieza a masificarse el uso de Internet dentro de las organizaciones. Asimismo, comienza a aparecer información especializada en seguridad de la información, así como el desarrollo de herramientas y técnicas específicas para dicha función.

A la vez, comienza a escucharse en nuestro país, organizaciones a nivel mundial, tales como: Carnegie Mellon University, SANS, (ISC)² e ISACA, quienes ofrecían entrenamiento y certificaciones en tópicos relacionados con mejores prácticas, seguridad de la información y objetivos de control para la tecnología de información (tal es el caso de CobiT, Control Objectives for Information and related Technology).

En este punto, la seguridad de la información comenzaba a perfilarse como un elemento de apoyo estratégico al negocio, que permitía la creación de valor y aportaba elementos de control.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

¿Qué ha pasado desde los años 90's? (continuación)

Tecnológicamente, existían múltiples canales de atención y se procuraba la consolidación de datos, equipos y sistemas de aunado con el uso de esquemas únicos de autenticación y de gestión de usuarios. Surgen estándares de intercambio de información como XBRL, OFX, XML y VPN e infraestructuras de claves públicas y privadas. Existía además, una mayor utilización de los niveles de servicio como herramienta de gestión entre las unidades usuarias y la Función de Tecnología de Información.

En esta década, comienzan a gestarse los primeros planes de recuperación ante desastres (DRP, por sus siglas en inglés), y las prácticas relacionadas comenzaron su transición a la gestión de riesgos y contingencias dentro de la organización de TI, como medida de prevención

ante el inminente cambio del milenio. Estas actividades empezaron a permear lentamente al resto de las unidades de negocio, a medida que éstas comenzaron a reconocer la existencia de los riesgos operacionales asociados a la pérdida o interrupción de los sistemas.

Por otro lado, a finales de la década de los 90's, el fenómeno del Y2K comienza a forzar a las organizaciones a evaluar las vulnerabilidades en sus sistemas. Esto resultó en la definición de prácticas para el análisis de amenazas y vulnerabilidades, así como la evaluación y clasificación de riesgos.

Las organizaciones empezaron a considerar el rol del "Chief Information Security Officer" (CISO), y a reconocer su valor crítico para la organización, en la mitigación de los riesgos informáticos, los cuales eran principalmente para ese entonces: páginas Web fraudulentas, robo de sesiones y de identidad, sniffing,

accesos no autorizados y hurto de información sensible, entre otros.

Ya para ese entonces, la seguridad de información deja de verse sólo como un conjunto de vulnerabilidades conocidas y se establece la necesidad de un tratamiento constante y no de manera eventual, incorporándose un nuevo reto para las organizaciones: el cumplimiento.

Con la aparición de nuevas regulaciones como Gramm-Leach-Bliley Act, (GLBA, 1999), Sarbanes-Oxley (2002), Health Insurance Portability and Accountability Act Security Provision (HIPAA, 2003), las cuales imponían nuevos requerimientos en cuanto a seguridad y privacidad de la información, las organizaciones se vieron forzadas a definir e implantar controles de seguridad adicionales para garantizar el cumplimiento de las mismas, dándole más fuerza al rol del CISO.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

¿Qué ha pasado desde los años 90's? (continuación)

La figura del CISO fue adquiriendo cada vez más fuerza dentro de las organizaciones, a tal punto que comenzaron a surgir de forma natural, diversas modalidades de líneas de reporte, tal como se muestra en la Figura N° 5.

Para ampliar: haga click sobre la imagen

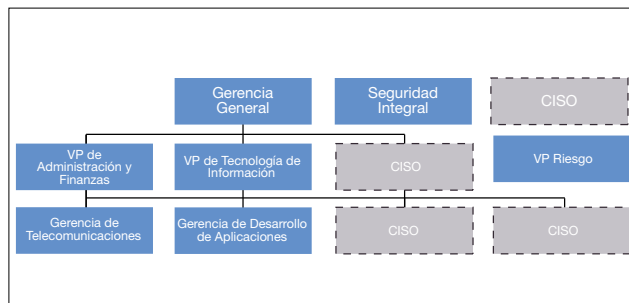


Figura N° 5. Estructuras propuestas del CISO a principios del milenio

Mientras tanto, el CISO continuó incrementando su entendimiento de los objetivos de negocio y aprendió una lección importante que le permitiría reducir o eliminar la práctica de generar Miedo, Incertidumbre y Duda (FUD, por sus siglas en inglés) para justificar sus presupuestos. Empezaron a tratar de utilizar el cálculo del Retorno de Inversión (ROI, por sus siglas en inglés), utilizando un cálculo derivado conocido como Retorno de Inversión en Seguridad de la Información (ROSI, por sus siglas en inglés) a lo largo de la cadena de administración de la infraestructura del negocio.

Sin embargo, aún cuando es notable la importancia que ha venido adquiriendo la seguridad de la información en las organizaciones, en el tema presupuestario, según los resultados obtenidos en la encuesta Nacional de las Prácticas de Seguridad de Información de las empresas en Venezuela, elaborada por Espiñeira,

Sheldon Asociados, Firma miembro de PricewaterhouseCoopers durante los períodos 2005 - 2006 y 2006 -2007, se establece que el presupuesto asignado para la Función de Seguridad de la Información, en proporción con el presupuesto de la Función de Tecnología de Información se encuentra entre el 2% y 10%, lo cual es un valor relativamente bajo si es comparado con la media mundial, que es de un 13% aproximadamente.

Esto nos permite inferir, que la seguridad, pese a la importancia adquirida, sigue presentando limitaciones para justificar su presupuesto, muy probablemente como consecuencia de la dificultad para demostrar el retorno de la inversión.

Contraloría, Auditoría y Riesgo:

Por su parte, las unidades de control también experimentaban algunos cambios con respecto a su alcance.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

¿Qué ha pasado desde los años 90's? (continuación)

Desde el punto de vista de estructura organizativa, ya se cuenta con una unidad formal de Contraloría con exigencias en el nivel académico del personal, mucho mayor que en las décadas anteriores. Empiezan a notarse mayores exigencias, hasta el punto que la mayoría de las organizaciones exige la contratación de contadores públicos colegiados. En cuanto a línea de reporte, Contraloría continúa adscrita a la Gerencia de Administración y Finanzas.

A nivel mundial, en septiembre de 1992 se publica el informe del Marco Conceptual Integrado de Control Interno - Estudio COSO I (ver Figura N° 6), y ante la ocurrencia de escándalos financieros ocurridos en la segunda mitad de la década de los noventa, la Comisión estudia la posibilidad de ampliar el estudio COSO I y considerar la

administración eficaz de los riesgos. Ello da origen a la publicación oficial de COSO II – ERM – GIR (ver Figura N° 8), en septiembre de 2004.

Para el sector financiero, en junio de 1999, el Comité de Basilea emitió una propuesta para un nuevo marco de adecuación de capital (que reemplaza el Acuerdo de 1988), el cual incorpora elementos necesarios para enfrentar las condiciones cambiantes del mercado, evolucionando hacia un esquema de requerimientos de capital que refleja con mayor precisión y sensibilidad, los riesgos asumidos.

Dicho Acuerdo lleva el nombre de Convergencia Internacional de Medidas y Normas de Capital: Marco Revisado – Basilea II.

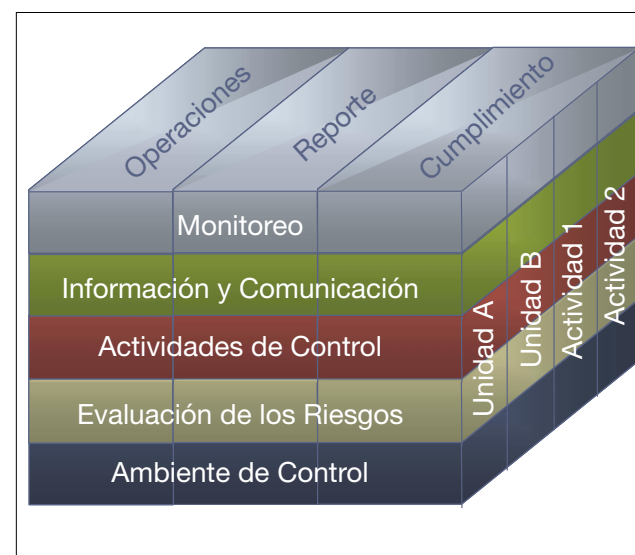


Figura N° 6. COSO I - Control Interno

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Las organizaciones del presente y futuro - ¿Qué está pasando actualmente?

El fin último de las organizaciones es alcanzar un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad, haciendo uso de la tecnología y asegurando la seguridad de la información a lo largo de las operaciones. El valor obtenido es maximizado, cuando la dirección establece las estrategias y objetivos para alcanzar un balance perfecto entre los objetivos de crecimiento, retornos y riesgos relacionados, utilizando de manera eficiente los recursos.

Todas las organizaciones se enfrentan a la incertidumbre presente en el camino para alcanzar sus metas. Esta incertidumbre incrementa los riesgos y oportunidades que pueden ser manejadas en función de aumentar el valor ganado.

La premisa principal de la administración corporativa de riesgos es que cada entidad, con o sin fines de lucro, existe para otorgar valor a sus grupos de interés. Todas las organizaciones encaran esta incertidumbre, es por ello que el desafío para la administración del negocio es

determinar cuanta incertidumbre está preparada para aceptar en la búsqueda de aumentar el valor (ver Figura N° 7). La incertidumbre proviene desde el entorno de las decisiones dentro de la organización y se puede presentar como un riesgo o una oportunidad, en función de destruir o crear valor.

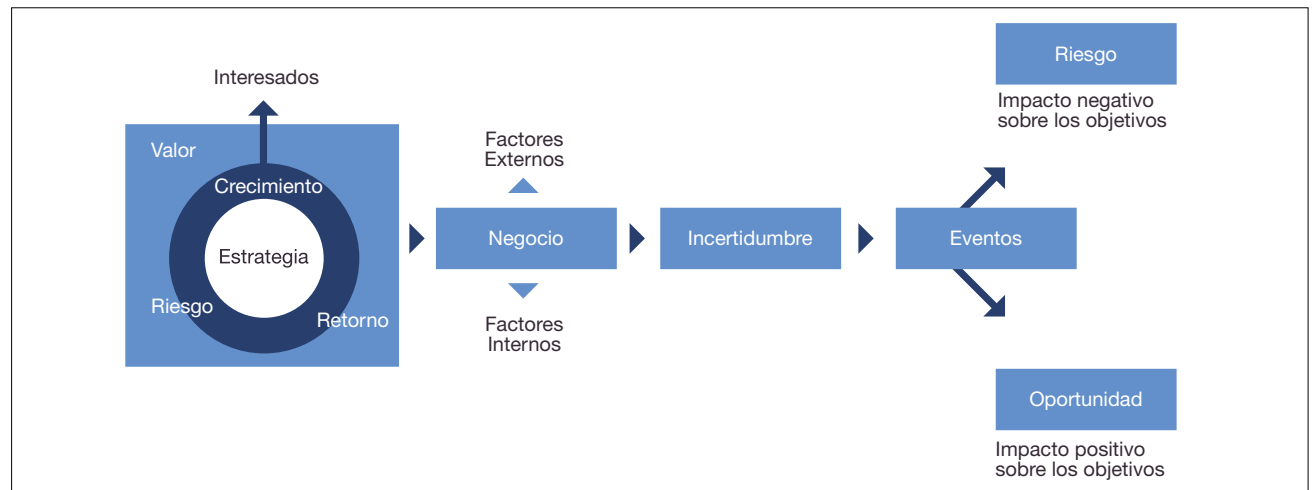


Figura N° 7. Premisas fundamentales de la administración corporativa de riesgos

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Las organizaciones del presente y futuro - ¿Qué está pasando actualmente? (continuación)

“La administración de riesgos corporativos es un proceso efectuado por el directorio, administración y las personas de la organización, es aplicado desde la definición estratégica hasta las actividades del día a día, diseñado para identificar eventos potenciales que pueden afectar a la organización y administrar los riesgos dentro de su apetito, a objeto de proveer una seguridad razonable respecto del logro de los objetivos de la organización”, según lo establece el Enterprise Risk Management – Integrated Framework COSO II del 29 de septiembre de 2004 (ver Figura N° 8).



Figura N° 8. COSO II - ERM (Marco de Gestión de Riesgo Empresarial)

Esta administración de riesgos permite a la organización manejar esa incertidumbre, su riesgo u oportunidad asociada y, por lo tanto, incrementar su capacidad para construir valor. En resumen, permite:

- Alinear la estrategia con el apetito al riesgo.
- Incrementar las respuestas al riesgo.
- Reducir las pérdidas y sorpresas operacionales.
- Identificar y administrar riesgos que cruzan la organización.
- Proveer respuestas integradas a múltiples riesgos.
- Identificar oportunidades.
- Mejorar la distribución de capital.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

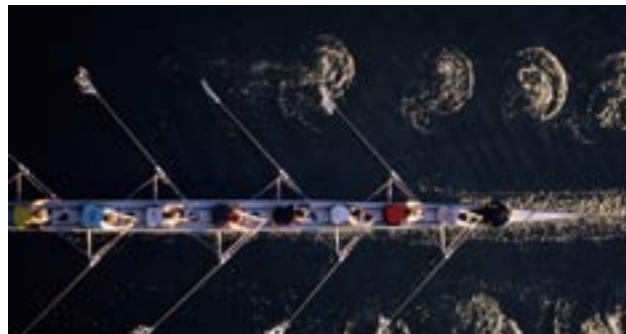
Las organizaciones del presente y futuro - ¿Qué está pasando actualmente? (continuación)

Este Marco de Gestión de Riesgo Empresarial (COSO II – ERM), se encuentra dirigido a lograr el aumento y eficiencia en las operaciones, la confiabilidad en los reportes financieros y alcanzar el cumplimiento de las leyes y regulaciones, que es hacia donde las organizaciones en el presente se están orientando. Puede decirse entonces, que el marco COSO II – ERM, se encuentra enfocado a cubrir los siguientes objetivos:

- Estratégico: Relacionado con las metas de alto nivel; asimismo están alineados y dan apoyo a la misión del negocio.
- Operacional: Relacionados con la efectividad y eficiencia de las operaciones de la organización, lo cual incluye su rendimiento y rentabilidad.

Usualmente, varían según las opciones adoptadas por la gerencia, en cuanto a estructura y rendimiento.

- Reporte o presentación de resultados: Relacionado con la confiabilidad y efectividad de la estructura de líneas de reporte.
- Cumplimiento: Relacionado con el apego de la organización a las leyes, regulaciones y políticas.



Necesidad de organizar la Gestión Integral de Riesgo

A continuación se describe una serie de situaciones generales que han sido identificadas, en el comienzo de la evolución de las organizaciones, relativas a los diagnósticos efectuados en los diseños de la Gestión Integral de Riesgo:

- Atomización de la Función de Gestión de Riesgo: en el enfoque tradicional de gestión de riesgo, era común encontrar funciones dispersas a lo largo de la organización. Por ejemplo, la unidad de Tesorería gestionaba los riesgos con enfoques y métodos diferentes a otras áreas de la organización.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Necesidad de organizar la Gestión Integral de Riesgo (continuación)

- Estructuras organizativas con problemas de independencia: el líder de la Unidad de Riesgo, cuando existía, reportaba a la Gerencia General, ocasionando posibles conflictos de intereses y potenciales riesgos éticos.
- Ausencia de Comité de Riesgo: carencia de un grupo colegiado, delegado por la Junta Directiva, para garantizar la gestión estratégica de los riesgos. Generalmente, este Comité se confundía con el Comité de Auditoría.
- Funciones de riesgo integradas en gestión de negocios: en la gestión de negocios era común encontrar funciones de Gestión de Riesgo cuya naturaleza era de control. Esto ocasionaba conflictos de interés, como por ejemplo en la función de “seguimiento de cartera de crédito”,

la cual se ubicaba como función en la gestión de negocios.

- Carencia de la Gestión de Riesgo Operacional: Auditoría Interna, por tradición, detectaba cierta categoría de riesgo operacional, utilizando metodologías con base en el Control Interno. Generalmente, no se incluía la fase metodológica de identificación de los riesgos y su ponderación.
- Visión limitada de los riesgos: ninguna unidad en las organizaciones tenía como misión la creación de una cartera de riesgos de diferente naturaleza, con el fin de visualizar de forma integral y gerencial las respuestas de una forma eficiente.
- Poca cultura de riesgo y control: actualmente, cuando se realizan mediciones de la cultura de riesgo y control, es frecuente encontrar

indicadores por debajo del promedio estándar del sector donde pertenecen las organizaciones. Muchas veces, se entiende el riesgo y el control, como la tradicional “alcabala” que frena el desarrollo del negocio y con una falta de relación con los objetivos estratégicos del negocio. En general, no existe una cultura de riesgo y control positiva.

Más allá de las iniciativas de las organizaciones que de manera proactiva tomaron acciones en función de formalizar la gestión de riesgos, gracias al surgimiento de mejores prácticas, normas y regulaciones internacionales y nacionales (tales como: COSO I, COSO II, Basilea I, Basilea II), para el caso de Venezuela, la Resolución 136.03 de la SUDEBAN (2003), se otorga un carácter institucional a la gestión de riesgo en las organizaciones. Es por ello que comienzan a surgir estructuras organizativas de la Unidad de Riesgo bajo dos (2) esquemas:

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Necesidad de organizar la Gestión Integral de Riesgo (continuación)

Centralizado o descentralizado.

Unidad de Gestión Integral de Riesgo

centralizada: existe un responsable de la Unidad de Riesgo, quien reporta al Comité de Riesgo. Existen además Oficiales de Riesgo reportando al responsable de riesgo. Bajo este enfoque, todas las funciones de riesgo pertenecen a la Gestión Integral de Riesgo, y las políticas, metodologías y procesos de riesgo están centralizados. Se delega la identificación de los riesgos en las Unidades de Negocios y la evaluación de control interno en Auditoría Interna. Adicionalmente, existe un rol de Oficial de Riesgo en las unidades de negocio y apoyo, el cual reporta a los gerentes funcionales de esas áreas (ver Figura N° 9).



Para visualizar la Figura No. 9 haga click en el icono.

Unidad de Gestión Integral de Riesgo

descentralizada: existe un responsable de la Unidad de Riesgo, quien reporta al Comité de Riesgo. Se descentralizan ciertas funciones de riesgo en las Unidades de Negocio, pero se establecen controles de seguimiento. Bajo este enfoque, se incrementan las funciones de delegados de riesgo y se descentraliza en las unidades de negocio la identificación y ponderación de los riesgos. Auditoría Interna evalúa el control interno, con base al riesgo (ver Figura N° 10).



Para visualizar la Figura No. 10 haga click en el icono.

Gobernabilidad en las organizaciones

El Gobierno Corporativo, tal como lo define el Dey Comittee y PricewaterhouseCoopers “es el proceso y estructura utilizado para dirigir y administrar el negocio con el objetivo de incrementar y sostener su valor. Dichos procesos y estructura deben definir una división de poder que conduzca al desempeño sostenible, promueva los comportamientos deseados y establezca los mecanismos necesarios para alcanzar la rendición de cuentas entre la gerencia, la Junta Directiva, los accionistas y los distintos grupos de interés de la empresa”.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Gobernabilidad en las organizaciones (continuación)

Bajo este enfoque, no basta con cumplir las normas y regulaciones: se requiere además cultura ética y buenas prácticas en los negocios, información transparente y adecuadamente expuesta y procesos apropiados para administrar y monitorear los riesgos. El Gobierno Corporativo no es un departamento, no es una división, es una pauta cultural. La ética y el buen Gobierno Corporativo no se declaran, simplemente se ejecutan.

Si analizamos el concepto de Gobierno Corporativo, y haciendo una analogía con el concepto de Gobernabilidad de TI, del IT Governance Institute, se establece: “es el conjunto de responsabilidades y prácticas ejercidas por la Dirección y la alta gerencia con el fin de proporcionar una dirección estratégica,

asegurando tanto el logro de los objetivos como el manejo adecuado de los riesgos y verificando que los recursos de la institución se utilicen de manera responsable” (ver Figura N° 11); es posible concluir que para alcanzar la “gobernabilidad”, la meta fundamental es lograr alinear la estrategia del negocio en función de garantizar el vínculo entre los planes de la organización y los planes y operaciones de las unidades de negocio. De esto se concluye que debe existir una propuesta de entrega de valor a lo largo del ciclo de entrega, asegurando que las Unidades de Negocio generen los beneficios prometidos en la estrategia, concentrándose en la optimización de los costos.

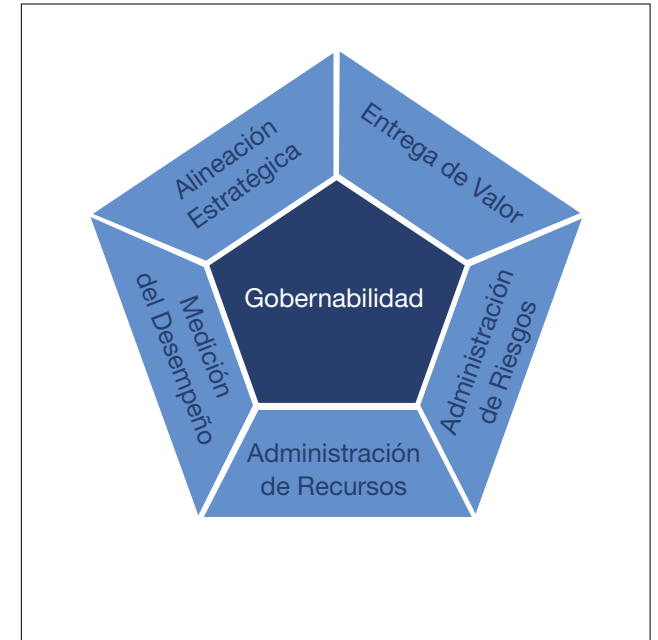


Figura N° 11. Modelo de Gobernabilidad de TI

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Gobernabilidad en las organizaciones (continuación)

En este sentido, la administración de los recursos se refiere a la inversión óptima, así como la administración apropiada de los recursos críticos de las unidades de negocio, tales como: las aplicaciones, información, infraestructura y las personas.

Adicionalmente, también debe contemplarse la administración integral de riesgos, logrando crear conciencia de los riesgos en la Alta Gerencia, un entendimiento claro del apetito de riesgo de la organización, requerimientos de cumplimiento y la definición de una estructura organizativa de administración de riesgo.

Asimismo, deben ser definidas herramientas y mecanismos para la medición del desempeño de la estrategia de implantación, terminación de proyectos, uso de recursos, desempeño de los procesos y entrega de valor de las unidades de negocio.

Sin embargo, podemos afirmar que entre las primeras actividades para alcanzar la gobernabilidad en las organizaciones, es requerida la definición de la estructura organizativa, líneas de reporte y la descripción de los roles y responsabilidades.

Roles y responsabilidades

Desde el punto de vista del control y gestión en las organizaciones, es necesario definir los roles y responsabilidades de los actores que deben alcanzar el consenso para alinear los diversos intereses involucrados para ejecutar el programa de negocio, logrando el balance óptimo entre los objetivos de crecimiento, retorno y riesgos relacionados, utilizando de manera eficiente los recursos (ver Figura N° 12). Entre los actores principales se encuentran:

- Comité de Riesgo.
- Unidad de Riesgo Integral.
- Unidad de Contraloría.
- Comité de Auditoría.
- Auditoría Interna.
- Función de Tecnología de Información.
- Función de Seguridad de la Información.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Roles y responsabilidades (continuación)



Para visualizar la Figura No. 12 haga click en el icono.

A continuación se describen las principales responsabilidades para cada uno de los roles clave que contribuyen con la gobernabilidad en las organizaciones:

Comité de Riesgo:

El objetivo de este comité es la administración, identificación, medición y mitigación de los riesgos a los cuales se encuentran expuestas las organizaciones. Entre sus principales responsabilidades están las siguientes:

- Aprobar y recomendar límites de exposiciones al riesgo dentro de las políticas globales del proceso de gestión integral de riesgo aprobadas por la Junta Directiva.
- Velar que el perfil de riesgo de la organización esté acorde con los lineamientos establecidos por la Junta Directiva.
- Supervisar el desempeño y cumplimiento de los objetivos de la Unidad de Riesgo Integral, las herramientas de gestión de riesgo y cualquier otro aspecto relevante relacionado con la gestión de riesgo.
- Establecer políticas de riesgo para la organización, de acuerdo con los lineamientos fijados por la Junta Directiva.

Unidad de Riesgo Integral:

La Unidad de Riesgo Integral, estará bajo la supervisión y dirección del Comité de Riesgo, la cual para desarrollar sus funciones deberá:

- Velar por el cumplimiento de los límites de exposición al riesgo de los niveles de aprobación delegados para operaciones que involucren toma de riesgos.
- Analizar y hacer seguimiento del perfil de riesgo y de los indicadores de riesgo en las unidades de la organización.
- Diseñar, desarrollar, proponer modificaciones y mantener actualizadas las políticas para la gestión integral de riesgo.
- Informar periódicamente al Comité de Riesgo acerca del cumplimiento de metas y objetivos en relación con la gestión integral de riesgo.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Roles y responsabilidades (continuación)

- Someter a consideración del Comité de Riesgo, los resultados obtenidos en la cuantificación de las exposiciones al riesgo y las recomendaciones para su adecuada administración.
- Apoyar el Comité de Riesgo en el diseño de las estrategias de gestión de riesgo integral.
- Revisar los planes de implantación de las estrategias de gestión de los riesgos.
- Revisar periódicamente las exposiciones con los principales clientes, sectores económicos de actividad, áreas geográficas y tipos de riesgo.
- Velar, supervisar y controlar el cumplimiento y aplicación de políticas, límites y metodologías para la gestión de los riesgos.

Unidad de Contraloría:

Un Contralor es una persona quien supervisa la contabilidad y los reportes financieros dentro de una organización. Normalmente, la posición de Contralor la ocupa un contador público, quien debe asegurarse que exista un adecuado sistema de control interno. En este sentido las principales responsabilidades de un Contralor, son las siguientes:

- Preparar y publicar los estados financieros y los indicadores, correcta y oportunamente.
- Presentar los estados financieros a la Junta Directiva, periódicamente (al menos mensualmente, antes de su publicación).
- Ser el responsable de la función de control de presupuesto de inversiones y gastos.

- Participar activamente en la definición de la estructura contable de las transacciones, tanto para las operaciones regulares como de los nuevos productos.
- Asegurar la existencia de un sólido sistema de control interno.
- Participar activamente en la estructuración de las operaciones de alto impacto para los resultados de la organización. Por lo que debe establecer adecuados canales de comunicación con los responsables de las diferentes áreas de negocio.
- Responsable por la emisión oportuna de los reportes a los diferentes entes reguladores. En los casos que existan reportes que deben ser enviados por otras unidades de negocio, debe supervisar la integridad y oportunidad de la información a ser enviada.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Roles y responsabilidades (continuación)

- Ser el enlace con los organismos reguladores.
- Ser el enlace con los auditores externos y coordinar el desarrollo del trabajo.
- Ser el responsable por el cumplimiento de los aspectos fiscales (ISLR e impuestos municipales).
- Representar a la organización en cuanto a los temas contables ante los organismos regulatorios cuando sea requerido.
- Ser miembro de los Comités donde sea estipulado por los organismos reguladores. Su participación en otros Comités, será de apoyo y no debe tener voto.

Comité de Auditoría:

El Comité de Auditoría es parte esencial en el proceso de información corporativa. Su responsabilidad primaria es supervisar, en nombre de la Junta Directiva, la integridad de los controles en la información financiera y los procesos implantados por la gerencia para proteger el interés de los accionistas y otras partes interesadas. Sus principales responsabilidades son:

- Asegurar la adecuación y efectividad de sistemas de gestión de riesgos y controles internos y cómo afectan los reportes financieros.
- Asegurar la adecuación y efectividad de los sistemas para la preparación de reportes financieros al mercado, estados financieros periódicos.

- Monitorear el cumplimiento de leyes y regulaciones, y su impacto en los resultados financieros.
- Monitorear el cumplimiento de los códigos de conducta, las denuncias y asegurar que se efectúen las investigaciones.
- Discutir con la Junta Directiva el perfil de riesgo y asegurar que la administración opere con base en los parámetros establecidos.
- Entender el marco de evaluación de riesgos, su gestión y la asignación de responsabilidades.
- Revisar las mayores exposiciones de riesgos financieros y la gestión de la gerencia para monitorearlos y controlarlos.
- Asegurar que existan controles sobre la integridad de los sistemas de contabilización y los registros contables.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Roles y responsabilidades (continuación)

- Asegurar que existan controles para asegurar presentación razonable y revelaciones de la información financiera.
- Hacer especial énfasis en los fraudes en cuanto a: su prevención, monitoreo y mitigación.
- Recabar información del Oficial de Cumplimiento, Consultor Jurídico o Gerente de Impuestos para alertarlos de temas que afecten a la organización.
- Brindar apoyo a la Junta Directiva y la gerencia en la adopción de Códigos de Ética y Conducta.

- Establecer o revisar los pasos dados por la gerencia para las líneas de denuncias a las faltas cometidas por los empleados (whistleblowing), los procesos de investigación y acciones tomadas.
- Establecer la coordinación de información con los siguientes Comités: Riesgo, Gestión de Ética y Conducta, Ejecutivo, entre otros.

Auditoría Interna:

Auditoría Interna tiene como propósito examinar, evaluar y monitorear la adecuación y efectividad del control interno de la organización. Siendo el Auditor Interno un empleado de la organización, es recomendable que su nivel de reporte sea al más alto nivel (Presidencia Ejecutiva o Junta Directiva) para que pueda ser lo más objetivo posible en sus evaluaciones y opiniones. El Auditor debe tener el máximo cuidado en el

- trabajo que realiza y en la elaboración de sus informes y conclusiones, las cuales deben estar presentadas con total imparcialidad y en forma objetiva. Dentro de las principales funciones del Auditor Interno, están las siguientes:
- Definir los objetivos, alcance y metodología para instrumentar la auditoría interna.
 - Captar la información necesaria para evaluar la funcionalidad y efectividad de los procesos, funciones, sistemas utilizados y controles implantados, la estructura y funcionamiento de la organización en todos sus ámbitos y niveles, así como los registros contables e información financiera.
 - Preparar y desarrollar el plan de auditoría interna para ejecutar la revisión de las áreas o procesos prioritarios según las evaluaciones realizadas.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Roles y responsabilidades (continuación)

- Detectar los hallazgos y evidencias e incorporarlos a los papeles de trabajo.
- Diseñar y preparar los reportes de avance e informes de auditoría interna.
- Proponer los sistemas administrativos y/o las modificaciones que permitan elevar la efectividad de la organización, así como proponer los sistemas y la tecnología de información de punta requerida para impulsar el cambio organizacional.
- Presentar los informes de auditoría interna al Comité de Auditoría.
- Apoyar al Comité de Auditoría en la ejecución de las actividades asignadas como parte de las

evaluaciones que se presenten y no consideradas en el plan de auditoría.

Función de Tecnología de Información:

La Función de Tecnología de Información es la unidad encargada de proveer la visión tecnológica y el liderazgo necesario para el desarrollo y la implementación de iniciativas informáticas que permiten mantener las ventajas competitivas de una organización, aplicando elementos de control establecidos principalmente, por las unidades de Auditoría Interna o Seguridad de la Información. Entre sus principales funciones se encuentran:

- Coordinar y gestionar los requerimientos de las áreas funcionales para diseñar una plataforma tecnológica que apoye los procesos del negocio.
- Evaluar la factibilidad de implantación de sistemas de información y aplicativos.

- Definir plataformas tecnológicas que se ajusten a las necesidades actuales y que sean escalables en un futuro.
- Negociar con los proveedores la adquisición de productos y servicios, así como, monitorear el cumplimiento de los mismos.
- Desarrollar, coordinar y ajustar, de ser necesario, las actividades asociadas a la planificación estratégica en tecnología de información.
- Dirigir, coordinar y evaluar los recursos humanos, tecnológicos y financieros necesarios para la ejecución de proyectos y mantenimiento a programas.

Boletín de Asesoría Gerencial

Cómo alcanzar la gobernabilidad en las organizaciones

Roles y responsabilidades (continuación)

Función de Seguridad de la Información:

La Función de Seguridad de la Información es la unidad encargada de proveer y mantener un modelo de seguridad que minimice los riesgos relacionados con la confidencialidad, integridad y disponibilidad de la información de la organización, acorde con los requerimientos, estrategias y planes del negocio; mejores prácticas y estándares internacionales. Entre sus principales funciones se encuentran:

- Crear las relaciones a nivel ejecutivo, gestión de los recursos centralizados de seguridad y la coordinación de los recursos descentralizados.
- Establecer las políticas, normas y procedimientos relacionados con la seguridad de la información.

- Dirigir y llevar la estrategia y programa a la seguridad.
- Coordinar la difusión de material educativo para concienciar a los usuarios en relación con los riesgos derivados de la tecnología de información.
- Dar soporte a los dueños de los recursos para desarrollar las políticas y mecanismos apropiados y para la aplicación de las mismas.
- Dar soporte al negocio mediante la gestión de accesos y privilegios de usuarios.
- Operar el monitoreo diario (auditorías operacionales) del estado de seguridad de información del negocio, investigación de vulnerabilidades, monitoreo, escaneo y otros.

Conclusión

Actualmente, existen grandes retos para las organizaciones, las cuales se encuentran enfocadas en la ejecución de procesos eficientes que les permitan alcanzar las metas trazadas y con un nivel aceptable de inversión, logrando compaginar esta relación, con la entrega de valor a los interesados.

Adicionalmente, hoy en día representa un desafío combinar la afirmación anterior, con el cumplimiento de las regulaciones orientadas a normar y formalizar el control y la gestión de los procesos de negocio, por lo que la implantación de las medidas de control y gestión, debe ser realizada sin llegar a confundir los roles y responsabilidades de cada uno de los actores principales de negocio tales como Auditoría, Riesgo, Contraloría, Tecnología y Seguridad. Sin duda esto contribuirá al éxito que pueda alcanzar una organización en su ambiente de control.

Boletín de Asesoría Gerencial

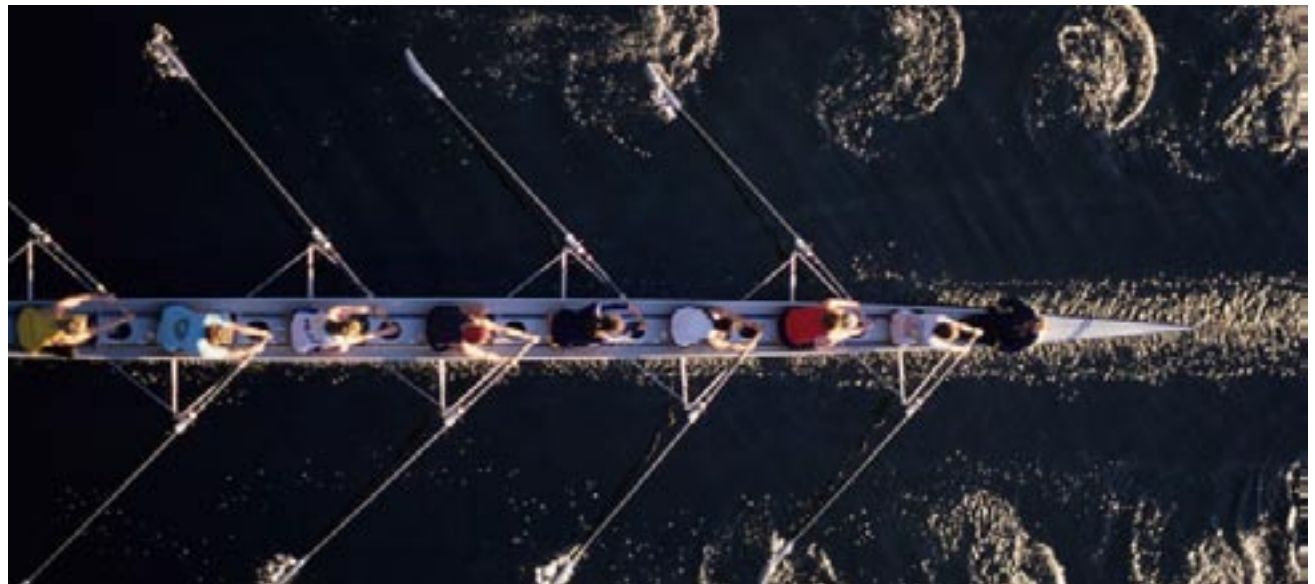
Cómo alcanzar la gobernabilidad en las organizaciones

Si desea suscribirse haga click en la barra

El Boletín Asesoría Gerencial es publicado mensualmente por la Línea de Servicios de Asesoría Gerencial (Advisory) de Espiñeira, Sheldon y Asociados, Firma miembro de PricewaterhouseCoopers.

El presente boletín es de carácter informativo y no expresa opinión de la Firma. Si bien se han tomado todas las precauciones del caso en la preparación de este material, Espiñeira, Sheldon y Asociados no asume ninguna responsabilidad por errores u omisiones; tampoco asume ninguna responsabilidad por daños y perjuicios resultantes del uso de la información contenida en el presente documento. *connectedthinking es una marca registrada de PricewaterhouseCoopers. Todas las otras marcas mencionadas son propiedad de sus respectivos dueños. PricewaterhouseCoopers niega cualquier derecho sobre estas marcas

Editado por Espiñeira, Sheldon y Asociados
Depósito Legal pp 1999-03CS141
Teléfono master: (58-212) 700 6666



© 2008. Espiñeira, Sheldon y Asociados. Todos los derechos reservados. "PricewaterhouseCoopers" se refiere a la firma venezolana Espiñeira, Sheldon y Asociados, o según el contexto, a la red de firmas miembro de PricewaterhouseCoopers International Limited, cada una de las cuales es una entidad legal separada e independiente. RIF: J-00029997-3

Figura N° 9. Unidad de Gestión de Riesgo Integral centralizada

Regresar al boletín Aumentar Imprimir

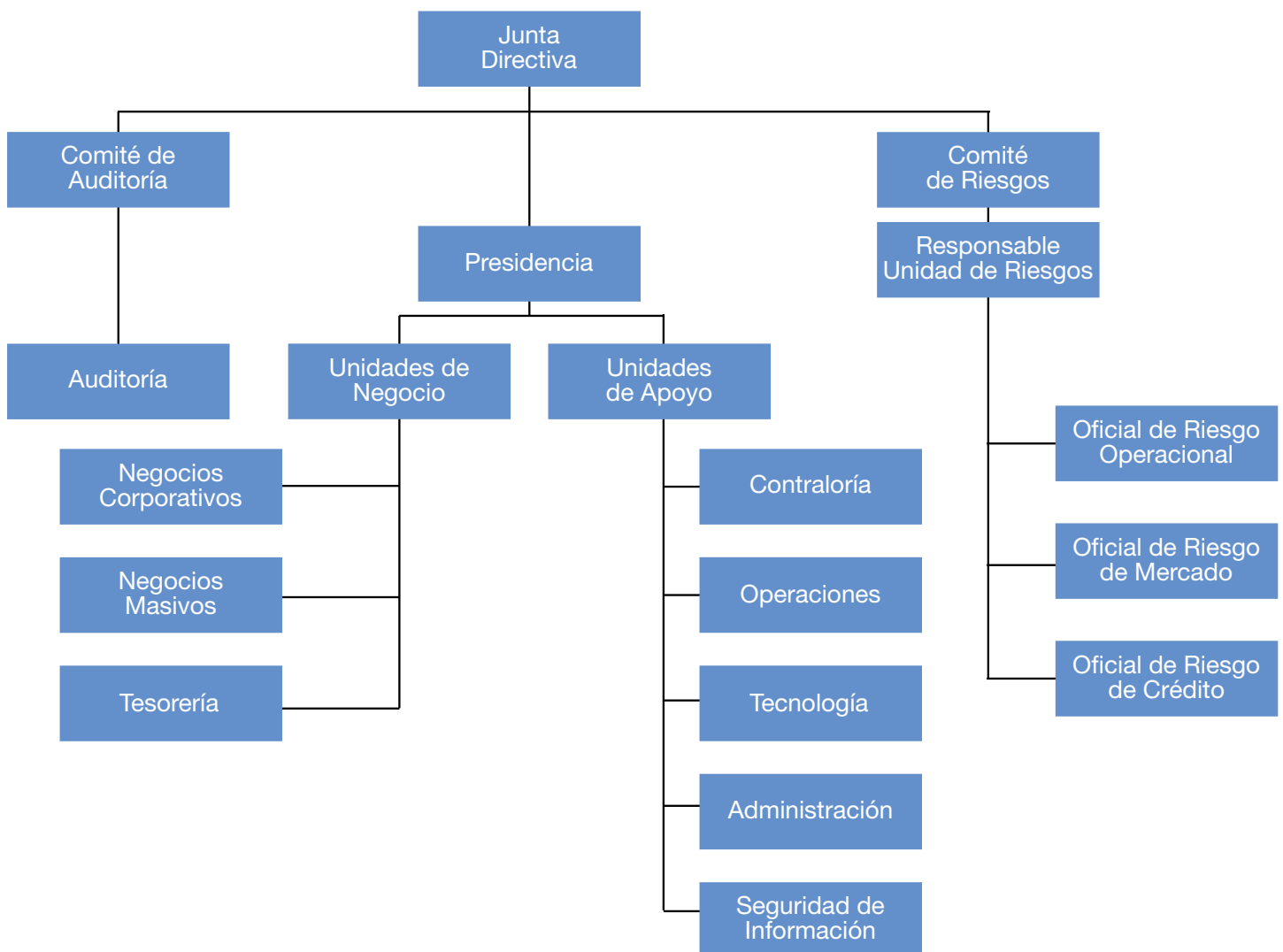


Figura N° 10. Unidad de Gestión de Riesgo Integral descentralizada

Regresar al boletín Aumentar Imprimir

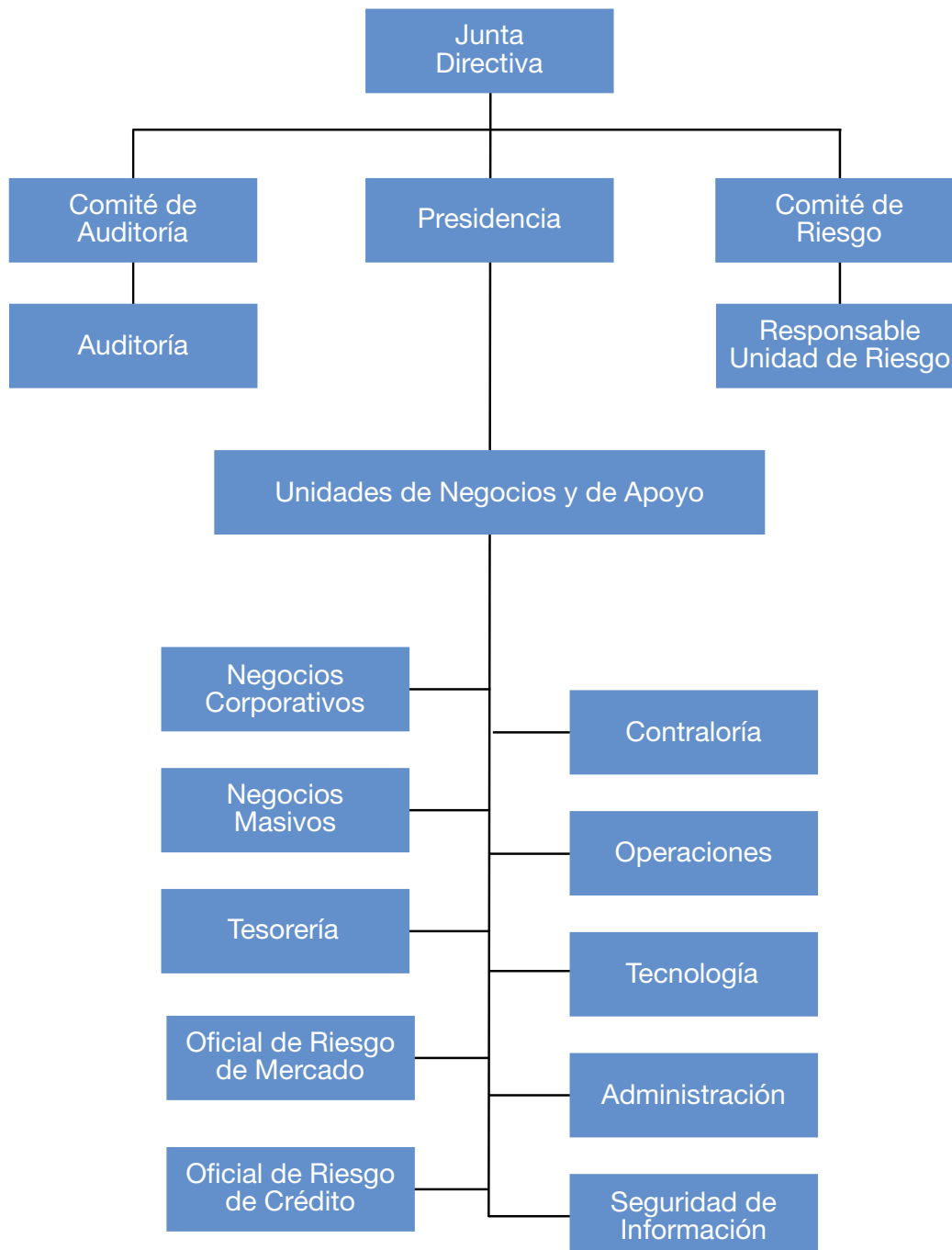


Figura N° 12. Principales actores y responsabilidades

Regresar al boletín Aumentar Imprimir

