Categorías de Objetivos:

1. Estratégicos
2. Operativos
3. De reporte, y
4. Cumplimiento.

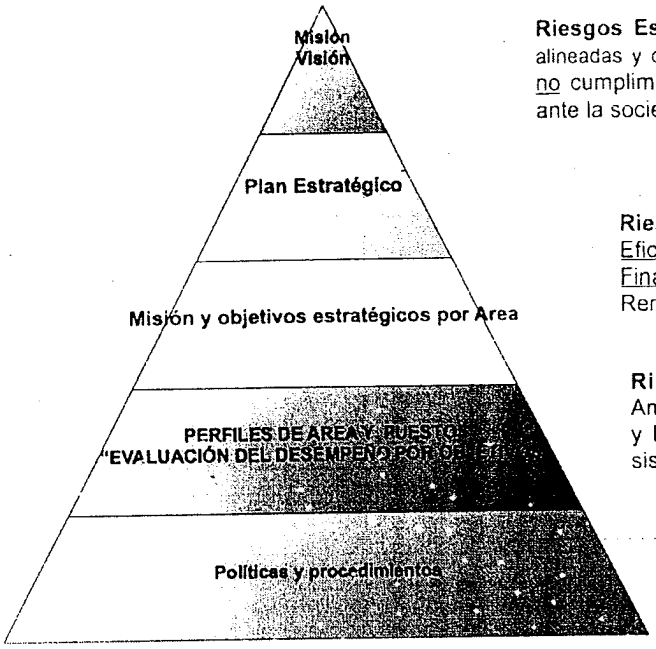
- **Estratégicos:**
  Se refieren a lo que se aspira alcanzar. Sea "misión", "visión", o finalidad.

- **Operativos:**
  Se refiere a la efectividad y eficiencia de las operaciones de la entidad, incluyendo objetivos de rendimiento y rentabilidad y salvaguarda de recursos frente a pérdidas.

- **De reporte:**
  Relativo a la confiabilidad de reportes. Incluyen reportes internos y externos y deben involucrar información financiera y no financiera.

- **De cumplimiento:**
  Se refieren al cumplimiento de leyes y regulaciones relevantes.

Los Riesgos y la Pirámide Empresarial



Riesgos Estratégicos: referidos a metas de alto nivel, alineadas y dando soporte a la misión / visión afectan el no cumplimiento y consistencia de ésta y su imagen ante la sociedad.

Riesgos Operacionales: vinculados al uso Eficaz y Eficiente de los Recursos y su efecto Financiero en las operaciones de la entidad. Rentabilidad y Productividad

Riesgos de Información / Financieros: Amenazan la Fiabilidad de la Información Interna y Externa para terceros y la generada por los sistemas de gestión.

Riesgos de Cumplimiento: Relacionados con la Legislación vigente. Y las políticas y procedimientos dictadas por la entidad.

Los 8 elementos del COSO ERM son los siguientes:

1. Ambiente de control
2. Establecimiento de objetivos
3. Identificación de eventos (riesgos)
4. Evaluación del riesgo
5. Respuesta al riesgo
6. Actividades de control
7. Información y comunicación
8. Supervisión (monitoreo)

1. Ambiente de Control

Es la base fundamental para los otros componentes del COSO ERM (Gestión de Riesgo Empresarial), dando disciplina y estructura. Incide en:

- **El modo en que las estrategias y objetivos son establecidos, las actividades del negocio son estructuradas e identifican y evalúan los riesgos, y actúa sobre ellos.**

- **Incide en la concientización del personal, respecto del riesgo y el control.**

- Influye en estrategia y objetivos, actividades de negocio, riesgos identificados, evaluación de riesgos y acciones sobre éstos.

- Influye en el diseño de actividades de control, sistemas de información y comunicación, y supervisión de actividades.

- Aquí es donde las metas establecidas por la Dirección, la filosofía, apetito y cultura de riesgo también emanados de la Dirección, integra a ERM con todas las actividades relacionadas.

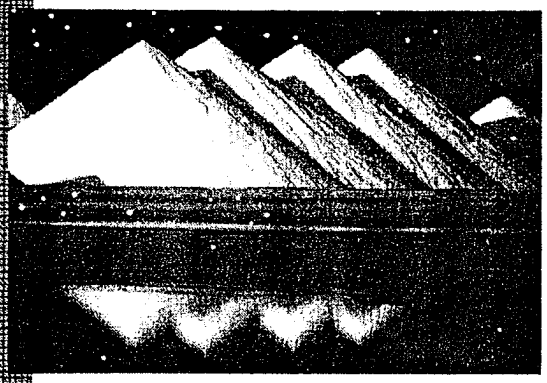
Componente COSO-ERM: Ambiente de Control

Enmarca el tono de la organización, influenciando la conciencia del riesgo en su personal.

Es la base del resto de los componentes y provee disciplina y estructura.

Este componente establece:

- Una filosofía de gestión integral de riesgo.
- Nivel de riesgo que la alta gerencia asume (Apetito de riesgo).
- El supervisor de la alta dirección en la gestión integral de riesgo.
- La integridad y los valores éticos.
- Los estándares, la gestión integral de riesgos, sistemas de delegación de autoridad, roles y responsabilidades y líneas de reporte.
- Estándares de recursos humanos: capacidad y competencia de los empleados.

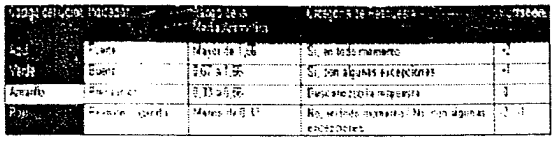


Ejemplo

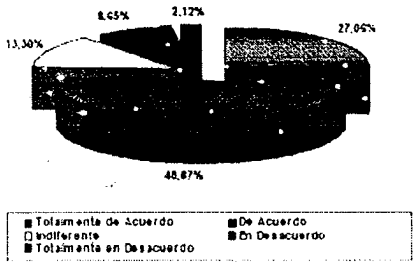
Filosofía de Gestión de Riesgo

MEDICIÓN DE CULTURA DE RIESGO Y CONTROL

- Identificación de áreas claves, niveles de cargos y personal que será sujeto a medición
- Distribución de cuestionarios e instructivos
- Recolección de cuestionarios
- Procesamiento, análisis y elaboración de informe
- Establecimiento de acciones estratégicas



Banco Z	Benchmarking Media Aritmética MCRC Instituciones Financieras del País		
	Más Baja	Promedio	Más Alta
0,90	0,90	1,12	1,22



2. Establecimiento de Objetivos:

Es la condición previa para la identificación de eventos, la evaluación de riesgos y la repuesta a ellos. Tienen que existir primero los objetivos para que la dirección pueda identificar y evaluar los riesgos que impiden su consecución y adoptar medidas para administrar dichos riesgos.

- Objetivos relacionados. (operativos, reporte, cumplimiento)
- Objetivos estratégicos. (misión, visión)

Componente COSO-ERM: Establecimiento de Objetivos

Dentro del marco de la definición de la misión y visión, la gerencia establece las estrategias y objetivos.

- La gestión integral de riesgo se asegura que la gerencia cuente con un proceso para definir objetivos que estén alineados con la misión y visión, con el apetito de riesgo y niveles de tolerancia
- Los objetivos se clasifican en cuatro categorías:
  - Estratégicos
  - Operacionales
  - Reporte o presentación de resultados
  - Cumplimiento

Objetivos operativos u operacionales:

Se corresponden con la efectividad y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y de salvaguarda de recursos frente a pérdidas.

Objetivos de reporte:

Relativos a la confiabilidad de reportes. Incluyen reportes internos y externos y deben involucrar la información financiera y no financiera.

Objetivos de cumplimiento:

Se refieren al cumplimiento de leyes y regulaciones relevantes. Dependen de factores externos y tienden a ser similares entre entidades, en algunos casos, y sectorialmente, en otros.

Ciertos objetivos dependen del tipo de negocio de la entidad. Ej: algunas empresas remiten información a agencias medioambientales y otras que cotizan en la bolsa, a los reguladores de los mercados de valores. Estos requisitos externos se establecen por leyes y regulaciones.

Establecimiento de Objetivos:

Los objetivos deben ser:

- **Alcanzables**
- **Medibles**
- **Orientados a resultados**
- **Realizables en un tiempo dado**
- **Específicos**

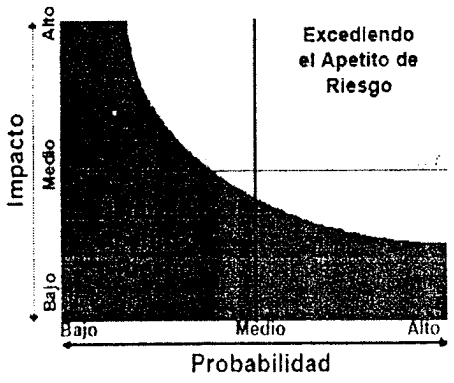
El tener objetivos no garantiza el éxito contra la competencia.

El éxito organizacional no se puede asegurar, aunque exista un buen desempeño.

Componente COSO-ERM: Establecimiento de Objetivos

Apetito de Riesgo

Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar



- Es una guía en el establecimiento de la estrategia
- La gerencia lo expresa como un balance entre: crecimiento, riesgo y retorno.
- Dirige la asignación de recursos
- Alinea la organización, personal, procesos e infraestructura

3. Identificación de Eventos - Riesgos:

Eventos: Son incidentes o acontecimientos, derivados de fuentes internas o externas, que afectan a la implementación de la estrategia o la consecución de objetivos. Pueden ser positivos o negativos, o de ambos tipos a la vez.

En otras palabras son las incertidumbres. Las que no se saben si ocurrirán, ni su impacto

Los eventos pueden tener efectos positivos, negativos, o ambos

- Negativo (riesgo): evaluar y formular respuesta
  - Lo importante es identificar los riesgos potenciales que pueden alejar a la empresa de la consecución de los objetivos estratégicos y operacionales
- Positivo (oportunidad): canalizarlo mediante estrategia administrativa y establecimiento de objetivos

	Grupo 1	Grupo 2	Grupo 3	Grupo 4
Evento 1			✓	
Evento 2	✓			
Evento 3	✓	✓	✓	✓
Evento 4				✓

Identificación de Eventos-Riesgos:

FACTORES EXTERNOS.

- Económicos
- Medioambientales
- Políticos
- Sociales
- Tecnológicos

Económicos: Cambios de precios, disponibilidad de capital, barreras a la entrada de la competencia, costos de capital y competidores nuevos.

Medio ambientales: inundaciones, incendios, terremotos, acceso restringido a materias primas o la pérdida de capital humano.

Políticos: elección de gobiernos nuevos, leyes, regulaciones que provocan nuevas restricciones.

Sociales: cambios demográficos, costumbres sociales, actividad terrorista, paros en la producción.

Tecnológicos: nuevos medios de comercio electrónico que generan mayor disponibilidad de datos.

FACTORES INTERNOS.

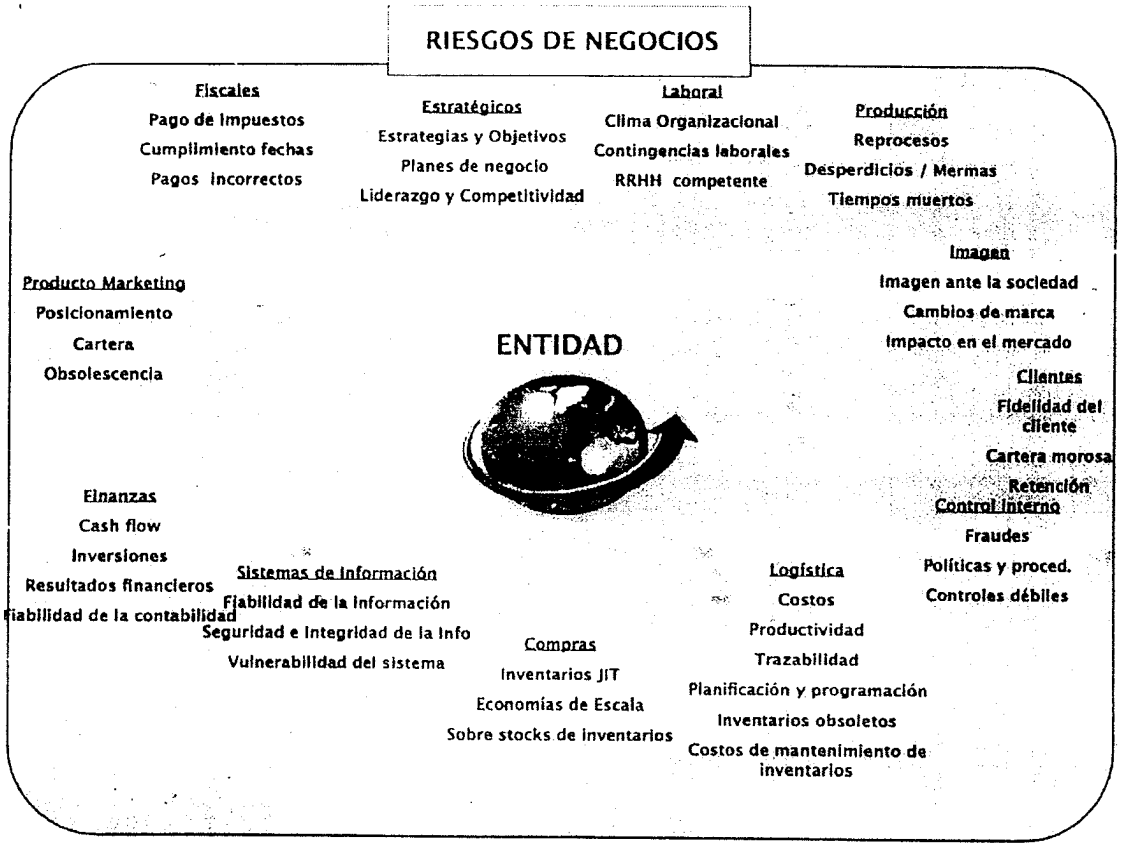
- Infraestructura
- Personal
- Procesos
- Tecnología

Infraestructura: Asignación de capital para mantenimiento preventivo y el apoyo a centros de atención de clientes para mejorar su satisfacción.

Procesos: Modificación de procesos, errores en su ejecución, pérdidas de cuotas de mercado, insatisfacción de cliente.

Personal: Incremento de Personal: accidentes laborales, actividades fraudulentas, vencimiento de convenios colectivos, daños reputacionales, paros en la producción.

Tecnología: Fallos de seguridad y la potencial caída de los sistemas dan lugar a atrasos en la producción, transacciones fraudulentas e incapacidad para continuar las operaciones del negocio.



4. Evaluación del Riesgo:

Permite a la entidad a considerar la amplitud con que los eventos potenciales impactan en la consecución de los objetivos.

- **Riesgo inherente: Al que se enfrenta en ausencia de acciones de la dirección para modificar su probabilidad.**

- Riesgo residual: Es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos.

Componente COSO-ERM: Identificación de Eventos

Se identifican eventos potenciales que si ocurren pueden afectar a la entidad. Base para los componentes evaluación de riesgos y respuesta al riesgo

- La gerencia reconoce que la incertidumbre existe, lo cual se traduce en no poder conocer con exactitud cuándo y dónde un evento pudiera ocurrir, así como tampoco sus consecuencias financieras

- En este componente se identifican los eventos con impacto negativo (riesgos) y con impacto positivo (oportunidades)

Formas de Evaluar los riesgos:

- **Tormenta (brainstorm) de ideas sobre riesgos y oportunidades**
- **Crear un Universo de Riesgos (inventario de riesgos)**
- **Identificar de raíz las causas y las correlaciones**
- **La mejor forma es tener sesiones de facilitación**
- **Calcular el impacto del riesgo usando la misma medida de los objetivos**
- **Calcular los escenarios mínimo, máximo y probable**
- **Preparar un mapa de riesgo (risk map)**
- **Priorizar riesgos y oportunidades basados en su valor ponderado**
- **Identificar los riesgos clave que requieren atención estratégica**

5. Respuesta a los riesgos:

Una vez evaluados los riesgos, la dirección determina cómo responder a ellos, (portafolio de riesgos).

- **Evitar: Supone salirse de las actividades que los generen.**

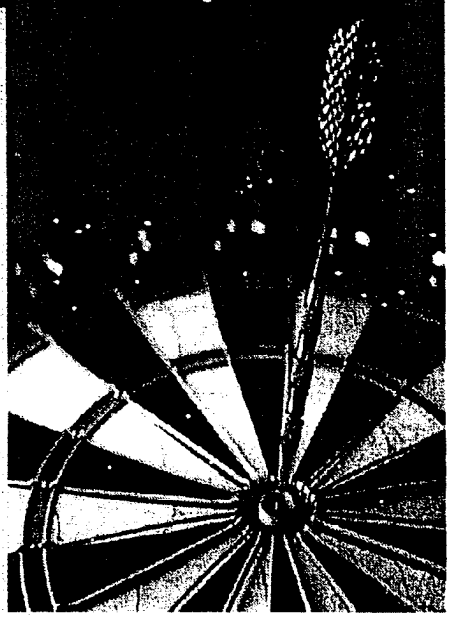
- Reducir: Es tomar decisiones para reducirlos.
- Compartir: Se reduce compartiendo el riesgo. (seguros)
- Aceptar: No se emprende ninguna acción.

Componente COSO-ERM: Respuesta al riesgo

Una vez identificados los riesgos, la gerencia determina como responderá ante ellos, a fin de alcanzar los niveles de tolerancia al riesgo

Las respuestas incluyen evitar el riesgo, mitigarlo, compartirlo o aceptarlo. En este sentido, la gerencia:

- Identifica y evalúa posibles respuestas al riesgo y el grado en el cual reducirá el impacto y/o probabilidad de ocurrencia
- Determina los costos y beneficios de las respuestas al riesgo que permitan ubicarlo dentro de los niveles de tolerancia deseados
- Identifica nuevas oportunidades de negocio para la organización

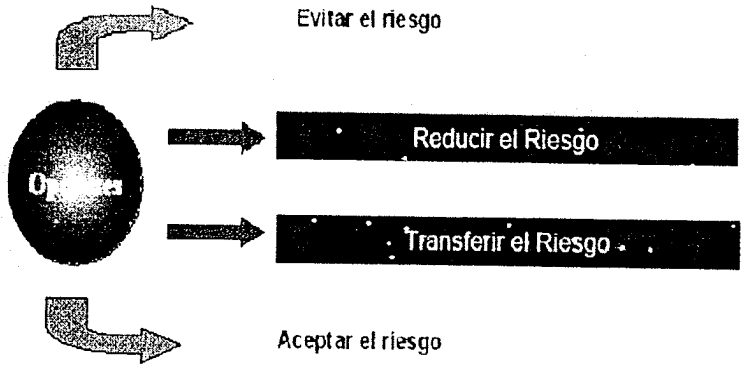


- Opciones y su efecto en la probabilidad e impacto de un evento
- Relación con: tolerancia al riesgo, costo versus beneficios
- Seleccionar respuestas que traerán la probabilidad e impacto de un evento dentro de la tolerancia al riesgo de la entidad
- Identificar y asignar responsabilidad para responder al riesgo
- Cuatro Tipos de Respuesta al Riesgo
-
  - Elusión
  - Compartir
  - Reducción
  - Aceptación
- **Redimensionar el riesgo sobre una base residual y desde una perspectiva de portafolio**
- **Algunos niveles de riesgo residual siempre existirán**

Componente COSO-ERM: Respuesta al riesgo

Evaluar posibles respuestas

Las respuestas deben ser evaluadas en función de alcanzar el riesgo residual alineado con los niveles de tolerancia al riesgo y pueden estar enmarcadas en las siguientes categorías:



6. Actividades de control:

Son las políticas y procedimientos que ayudan a asegurar que ya no se van a dar dichos riesgos (Controles internos preventivos, controles sobre sistemas de información, y controles generales).

- **Las políticas y procedimientos que ayudan a asegurar las respuestas al riesgo se llevan a cabo adecuadamente.**
  - **Política: Qué debe hacerse**
  - **Procedimiento: Cómo debe hacerse**
- **Parte del proceso de lograr los objetivos del negocio**
- **Importancia de los sistemas de información**
  - **Controles generales: aseguran que los sistemas trabajan apropiadamente, infraestructura, seguridad, compras de software, licencias, desarrollo y mantenimiento, reportes de actividades.**

- Controles de aplicaciones: aseguran la integridad, exactitud, autorización, validez de la captura de datos y proceso de transacciones, interfases de datos.

Componente COSO-ERM: Actividades de Control

Tipo de Actividades de Control	
Revisiones de desempeño del negocio	Comparaciones del desempeño versus presupuesto, proyecciones y desarrollo del período anterior Por ejemplo: La revisión de informes (por sucursal, región y tipo de préstamo) que realiza un gerente de crédito de un banco para aprobaciones y cobranzas
Controles físicos	Incluye resguardo de instalaciones, activos físicos, control de acceso físico, conteo periódico y comparación con lo registrado en el sistema Por ejemplo: Realización de inventarios físicos para la verificación de mercancías en stock con las cantidades presentadas en los sistemas de información
Segregación de funciones	Asignar a diferentes personas las responsabilidades de autorizar, registrar las transacciones y mantener la custodia de los activos Por ejemplo: Un vendedor no puede tener autorización para modificar precios de ventas o descuentos de los productos en el sistema

Componente COSO-ERM: Actividades de Control

Tipo de Actividades de Control

Controles sobre los sistemas de información

Controles de aplicación	**Enfocados en el cumplimiento de los objetivos del procesamiento de la información sobre integridad, exactitud, validez y acceso restringido Por ejemplo: Chequeos de existencias y de verificación de cálculos**
Controles generales	**Incluyen controles sobre la gerencia de tecnología de información, infraestructura de TI, seguridad de los activos de información, adquisición, desarrollo y mantenimiento de software**

Ejemplo

- Desarrollo e implantación: Asegurar que se desarrollen, configuren e implanten los sistemas para satisfacer los objetivos de la información financiera
- Mantenimiento: Asegurar que los cambios o modificaciones a los sistemas se realicen de forma adecuada, utilizando ambientes de desarrollo y producción separados, autorizaciones, documentación, pruebas, aprobaciones y análisis de impacto del cambio en otros sistemas o bases de datos
- Seguridad de la información: Asegurar que se autentifique y autorice el acceso a los recursos de los sistemas y datos

Componente COSO-ERM: Actividades de Control

Tipo de Actividades de Control

Diferentes diferentes tipos de controles:

Controles preventivos	Diseñados para evitar riesgos, errores o incidentes antes de su ocurrencia
Controles detectivos	Diseñados para detectar de forma rápida riesgos, errores o incidentes
Controles correctivos	Diseñados para remediar o reducir daños como consecuencia de riesgos, errores o incidentes ocurridos

Componente COSO-ERM: Actividades de Control

- Están presentes en todos los niveles y áreas funcionales de la organización para lograr los objetivos del negocio
- Incluye un rango de actividades, tales como:
  - Aprobaciones
  - Autorizaciones
  - Verificaciones
  - Conciliaciones
  - Seguridad de los activos
  - Desempeño de las operaciones
  - Segregación de funciones

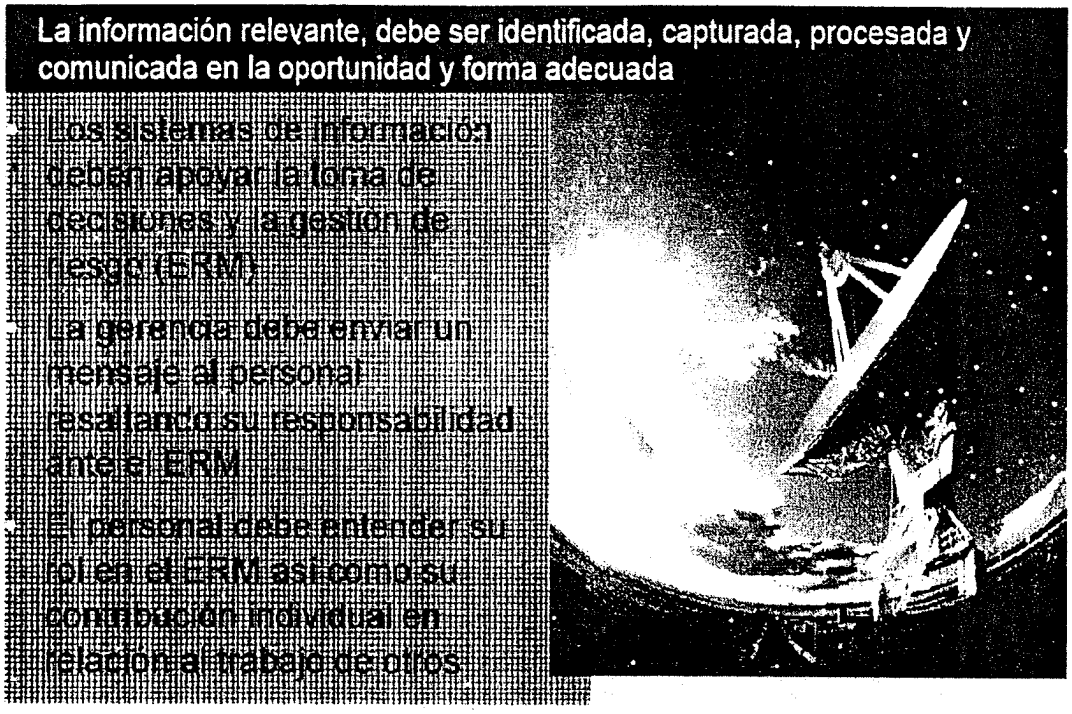
7. Información y Comunicación:

- **La información es necesaria en todos los niveles de la organización para identificar, evaluar y dar respuesta al riesgo.**
- **Se debe identificar, capturar y comunicar en tiempo y forma que permita al personal cumplir con sus responsabilidades. La información relevante es obtenida de fuentes internas y externas.**
- **La comunicación se debe realizar en sentido amplio y fluir por toda la entidad en todos sentidos.**
- **Debe existir una comunicación adecuada con partes externas a la organización como clientes, proveedores, reguladores y accionistas.**

- **De fuentes internas y externas**
- **Identifica, captura, analiza y comunica a quienes lo necesitan**
- **Forma y tiempo**
- **Útil para llevar a cabo responsabilidades**

- Fluye hacia abajo, hacia arriba y a lo largo de la organización
- Intercambio con partes externas: clientes, proveedores, legisladores, accionistas
- Útil para identificar, evaluar y responder a riesgos, mover la entidad y lograr los objetivos

Componente COSO-ERM: Información y comunicación



8. Supervisión o Monitoreo:

La Administración de Riesgos Corporativos de una entidad cambia con el tiempo. Las respuestas a los riesgos que antaño eran efectivas pueden llegar a ser irrelevantes; por lo tanto tienen que revisarse constantemente. Se puede realizar a través de:

- Actividades permanentes
- O mediante evaluaciones independientes.

A través de actividades permanentes.

Son los directores de línea o función de apoyo quienes llevan a cabo las actividades de monitoreo y dan meditada consideración a las implicaciones de la información que reciben. Ej. Aprobación de

transacciones, reconciliaciones de cuentas de balance y la verificación y exactitud de los cambios en archivos maestros.

Mediante evaluaciones independientes

Componente COSO-ERM: Monitoreo

El ERM es monitoreado, evaluando la presencia y funcionamientos de sus componentes a lo largo del tiempo

La eficacia de los otros componentes del ERM se sigue mediante:

- Actividades de supervisión continua
- Evaluaciones separadas

- Verificar que los componentes están presentes y funcionando
- Verificar su calidad en el curso del tiempo
- Dos caminos: Evaluaciones sobre la marcha o separadas
- La documentación varía: tamaño y complejidad de la organización
- La falta de documentación no significa que los componentes no existan o no puedan ser probados. La documentación hace que la supervisión sea más efectiva y eficaz
- Reportar las deficiencias a quienes pueden tomar la acción apropiada

Roles y Responsabilidades de la administración de riesgos corporativos:

- **Todo el personal en una entidad tiene algún tipo de responsabilidad en la administración de riesgos.**
- **El marco integrado de administración de riesgos de COSO ERM trata los siguientes roles internos y sus responsabilidades.**

- **Directorio**
- **Gerencia**
- **Oficial de riesgo**
- **Gerentes financieros**
- **Auditores internos**
- **Resto del personal**

Grupo	Responsabilidades
Consejo de Directores:	Dirección, Estrategia, Tono en la Cumbre, Riesgo, Apetito, Respuestas de ERM y del Riesgo
Administración	Dueños de ERM, tono en la cumbre, liderazgo, delegar responsabilidades apropiadamente, influencia a lo largo de unidades múltiples
Funcionario del Riesgo	Mantener una administración eficaz del riesgo, supervisar avances, reportar información relevante
Auditores Internos	Supervisar ERM y la calidad del desempeño. Asesorar a la administración, al consejo y al Comité de Auditoría, supervisando, revisando, evaluando, reportando y recomendando mejoras

ERM es responsabilidad de cada uno.
Todos los empleados utilizan, producen o tienen información útil en ERM.
Tomar acciones para administrar eventos y riesgos.

También trata el rol de los terceros a la organización, ya que proveen información útil para una adecuada administración:

- **Auditores internos.**
- **Legisladores y reguladores**
- **Clientes, proveedores.**
- **Analistas financieros,**
- **Medios de comunicación.**

Eficacia de COSO ERM

- **Un estado o condición en un momento dado**
- **Eficacia: todos los ocho componentes están presentes y funcionando**
- **Puede haber diferencias entre entidades, industrias y combinaciones de componentes. Diferencias debido a culturas diferentes, tamaño, industria, filosofía.**
- **Conceptos aplicables a todas las entidades sin importar su tamaño.**
- **Diferentes niveles de formalidad.**

- Deben considerarse las relaciones externas (inversión conjunta, asociaciones) que no están bajo un control directo.

1.4 Importancia e Independencia de la Auditoría Interna:

Importancia:

La auditoría interna es un instrumento de medición y evaluación de lo efectivo de la estructura de control interno de una entidad, contribuye con ésta para alcanzar los objetivos básicos, mencionados anteriormente.

Roles Críticos de la Auditoría Interna:

- Proporcionar seguridad en los procesos de gestión de riesgo
- Proporcionar seguridad de que los riesgos están siendo evaluados correctamente
- Evaluar los procesos de gestión de riesgo
- Evaluar los informes de los riesgos clave
- Revisar el manejo de los riesgos claves identificados

Roles que la Auditoría Interna puede realizar:

- Facilitar la identificación y evaluación de los riesgos
- Entrenar a la gerencia en responder a los riesgos
- Coordinar las actividades de Gestión de Riesgo Empresarial (ERM)
- Consolidar el informe sobre los riesgos
- Mantener y desarrollar el Marco de Gestión de Riesgo Empresarial (ERM)
- Promocionar el establecimiento de Gestión de Riesgo Empresarial (ERM)
- Desarrollar la estrategia de Gestión de Riesgo Empresarial (ERM) para la aprobación de la Junta Directiva

Roles que la Auditoría Interna no debe realizar:

- Fijar el nivel de riesgo aceptable
- Imponer procesos de manejo de riesgo
- Representar a la gerencia en relación a riesgos
- Tomar decisiones en relación a respuestas relativas a riesgo
- Implementar, a nombre de la gerencia, respuestas con relación a riesgos
- Responsabilidad en el manejo de riesgos

Independencia de la Auditoría Interna:

Para que la auditoría interna funcione bien debe tener dos características:

- Nivel organizacional
  El departamento de Auditoría Interna debe estar ubicado adecuadamente para que le permita el cumplimiento de sus responsabilidades y así lograr sus objetivos.

- Objetividad
  Al realizar cada trabajo de auditoría los Auditores Internos deben mantener una actitud mental positiva y objetiva y no permitir influencias por juicios de otras personas.

Ubicación de Auditoría Interna en el Organigrama

EMPRESA LA CHABELA, S. A.