# UNIDAD NO. 2

**LA ACTIVIDAD DE LA AUDITORÍA INTERNA, OBJETIVOS, ALCANCE, NATURALEZA, IMPORTANCIA E INDEPENDENCIA.**

- 1.1 Objetivos y alcance del trabajo de Auditoría Interna
- 1.2 Naturaleza de la Auditoría
- 1.3 Importancia e independencia de la Auditoría Interna

# 1.1 OBJETIVOS DE AUDITORÍA INTERNA

- El objetivo principal es ayudar a la alta dirección en el cumplimiento de sus funciones y responsabilidades, proporcionándole análisis objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas. Este objetivo se cumple a través de otros más específicos como los siguientes:

# Objetivos de Auditoría Interna

- Verificar la confiabilidad o grado de razonabilidad de la información contable y extracontable, generada en los diferentes niveles de la organización.
- Vigilar el buen funcionamiento del sistema de control interno (lo cual implica su relevamiento y evaluación) tanto del sistema de control interno contable como el operativo.

# Objetivos de Auditoría Interna

- La Auditoría Interna forma parte del Control Interno, y tiene como uno de sus objetivos fundamentales el perfeccionamiento y protección de dicho control. Por lo tanto los objetivos del control interno se han utilizado para contarlos como objetivos de Auditoría Interna y son los siguientes:

# Objetivos de Auditoría Interna

**OBJETIVOS:**

- Confiabilidad e integridad de la información.
- Cumplimiento de objetivos, políticas, planes, procedimientos, leyes y reglamentos.
- Salvaguardar los activos.
- Uso eficiente y económico de los recursos.
- Cumplimiento de objetivos y metas establecidas para las operaciones y programas.

# Objetivos de Auditoría Interna

**Confiabilidad e integridad de la información**:

El sistema de información proporciona datos que sirven para la toma de decisiones y para medir el control de las operaciones. Por lo tanto se debe verificar la confiabilidad e integridad de la información.

# Objetivos de Auditoría Interna

**CUMPLIMIENTO DE POLÍTICAS, PLANES, PROCEDIMIENTOS, LEYES Y REGLAMENTOS**:

La gerencia es responsable del establecimiento de sistemas para asegurarlos. Y la Auditoría Interna, es responsable de revisar y determinar si los sistemas son adecuados y efectivos y si las áreas auditadas cumplen los requerimientos.

# Objetivos de Auditoría Interna

**Salvaguarda de activos:**

Los auditores internos deben revisar la existencia y propiedad de los A/F utilizando procedimientos adecuados, y revisar los métodos de salvaguardas, si son apropiados para protegerlos y contrarrestar cualquier tipo de riesgo.

# Objetivos de Auditoría Interna

**Uso económico y eficiente de los recursos:**

El Auditor Interno debe evaluar si el empleo de los recursos mediante estándares de operación establecidos por la Admón. Se realizan en forma económica y eficiente.

# Objetivos de Auditoría Interna

**Uso económico y eficiente de los recursos debe identificar:**

- Sub utilización de instalaciones.
- Trabajo no productivo.
- Deficiente segregación de funciones.
- Procedimientos que no justifican el costo conforme estándares establecidos.
- Sub utilización de activos

# Objetivos de Auditoría Interna

**Cumplimiento de objetivos y metas establecidas para las operaciones y programas:**

- La administración es responsable de los objetivos, políticas, planes y procedimientos y el logro de los resultados de operación.
- A la Auditoría Interna le corresponde verificar el cumplimiento de lo establecido por la Admón. Y de ser necesario, proporcionar apoyo en el diseño y desarrollo previo a su implantación.

# 1.2 ALCANCE DEL TRABAJO DE AUDITORÍA INTERNA

- El alcance de la auditoría interna debe incluir la revisión y evaluación de la estructura del control interno implementado por la Administración de la Empresa, para determinar si el mismo es efectivo y eficiente.

# Alcance de la Auditoría Interna

- El alcance abarca la ejecución del plan de trabajo. Sin embargo, la Gerencia y el Consejo de Administración proporcionan una dirección sobre dicho alcance.
- El propósito de la revisión del Control Interno es determinar si se cumplen los objetivos del mismo.

# 1.3 NATURALEZA DE LA AUDITORÍA INTERNA

- Función de la Auditoría Interna.
- La Auditoría Interna como elemento de control.
- Ubicación de la Auditoría Interna en la estructura organizacional.

# 1.3 Identificación y análisis de riesgo

Se deben identificar los riesgos relevantes que enfrenta una empresa en la persecución de sus objetivos, ya sean de origen interno como externo.

# 1.3 Identificación y análisis de riesgo

Su desarrollo debe comprender la realización de un "mapeo" del riesgo, que incluya la especificación de los dominios o puntos claves de la empresa, la identificación de los objetivos generales y específicos, y las amenazas y riesgos que se pueden afrontar.

# 1.3 Identificación y análisis de riesgo

- Un dominio o punto clave de la empresa, puede ser:
- Un proceso que es crítico para su sobrevivencia;
- Una o varias actividades que sean responsables de la entrega de porciones importantes de servicios a la ciudadanía;

# 1.3 Identificación y análisis de riesgo

- Un área que está sujeta a leyes, decretos o reglamentos de estricto cumplimiento, con amenazas de severas puniciones por incumplimiento;
- Un área de vital importancia estratégica para el Gobierno (ejemplo: defensa, investigaciones tecnológicas de avanzada).

# 1.3 Identificación y análisis de riesgo

Por tal razón, se cambió el enfoque de la auditoría interna hacia el pasado por un enfoque hacia situaciones presentes y futuras, a través del análisis de detalles y hechos del pasado.

# 1.3 Identificación y análisis de riesgo

Dicho enfoque esta sobre la base de riesgos presentes y sobre futuras transacciones, el auditor está trabajando en un nivel que está por encima de los detalles y se proyecta hacia la generación de recomendaciones de alto valor agregado".

| | AI Historia | Intermedio Internal Audit | Auditoría a la vanguardía |
|---|---|---|---|
| Enfoque | Basada en plan rotativo | Prioriza basado en riesgos | En las estrategias y riesgos de procesos y negocios |
| Perspectiva | Historia | Historico – investigación de campo, dispara al herido | Futuro – ayuda al herido, mapeo de campos minados o evitar batallas |
| Estilo | Policía corporativo | El padre que todo lo sabe | Consultor y asesor |
| Mandato | Cumplimiento con politicas y proc | Aseguramiento en controles finac, cumpl | Aseguramiento del negocio |
| Enfoque riesgos | Financiero | Extra financiero | Riesgos empresariales |
| Herramientas | Prog. De trabajo de cumplimiento | Programas de audit para procesos y controles clave | Modelos de riesgos (COSO-ERM) autoevaluación |
| Tecnología | Ninguna | Papeles de trabajo automatizados | Pruebas automatizadas & Monitoreo continuo |
| Resultados | Pequeños hallazgos | Aseguramiento de areas clave | Proactiva admini de riesgo y reporte dinamico |

# 1.3 Identificación y análisis de riesgo

El auditor interno requiere desarrollarse en aspectos relacionados con la visión de los negocios, planeación con base en riesgos y habilidades de comunicación.

# 1.3 Identificación y análisis de riesgo

Es decir que actualmente el auditor interno debe moverse del tradicional enfoque financiero y contable hacia el enfoque de negocios y de sus riesgos asociados, considerando los aspectos financieros y contables como una parte del proceso de revisión y no como una finalidad de su trabajo.

| CARACTERÍSTICAS | ANTIGUO PARADIGMA | NUEVO PARADIGMA |
|---|---|---|
| Enfoque de la AI | Control Interno | Riesgos del negocio |
| Respuesta | Reactiva, posterior a los hechos. Observadores de las in iciativas del plan estratégico. | Proactiva, en tiempo real. Monitoreo continuo y participación en el proceso del plan estratégico. |
| Pruebas de AI | Importancia de los controles | Importancia de los riesgos |
| Métodos de AI | Énfasis en integridad de la evaluación d e controles detallados | Énfasis en la importancia de una significativa cobertura de los riesgos del negocio |
| Recomendaciones de AI | Controles Internos:<br>-Fortalezas/ debilidades<br>-Costo/beneficio<br>-Eficiencia/ efectividad | Manejo del riesgo:<br>-Evitarlos/diversifi cados<br>-Repartición/transferencia<br>-Controlarlos/aceptarlos |
| Informes de AI | Dirigidos hacia la funcionalidad de los controles. | Dirigidos hacia el proceso de riesgos. |
| Rol de la AI en la organización | Función de evaluación Independie nte de los controles intern os | Integración en el manejo del riesgo y comunicación constante con la Dirección. |

# Qué es riesgo?

Se produce riesgo cuando hay probabilidad de que algo negativo suceda o que algo positivo no suceda, la ventaja de una empresa es que conozca claramente los riesgos oportunamente y tenga la capacidad para afrontarlos.

# Qué es riesgo?

El Riesgo es un concepto que bien podría llamarse vital, por su vínculo con todo lo que se hace, casi podría decirse que no hay actividad de la vida de las personas, de los negocios o de cualquier actividad que se pueda desarrollar, que no incluya la palabra riesgo.

# Qué es riesgo?

Riesgo es la probabilidad de ocurrencia de un evento que pudiera afectar adversamente el logro de los objetivos de la institución.

Ninguna entidad opera en un ambiente libre de riesgos.

# Qué es riesgo?

Riesgo es cualquier obstáculo que se oponga al logro de los objetivos globales y específicos dentro de una organización.

Riesgo es una Situación adversa cuyas consecuencias para una organización es la pérdida de un activo (tangible o intangible).

El riesgo se mide en términos de impacto y probabilidad.

# Gestión de riesgo empresarial

Las empresas están expuestas a riesgos internos y externos. Algunos pueden ser estructurales, financieros, ambientales y operativos, etc.

Las empresas realizan actividades de gestión de riesgo para identificar, evaluar, manejar y controlar toda clase de eventos o situaciones.

# Gestión de riesgo empresarial

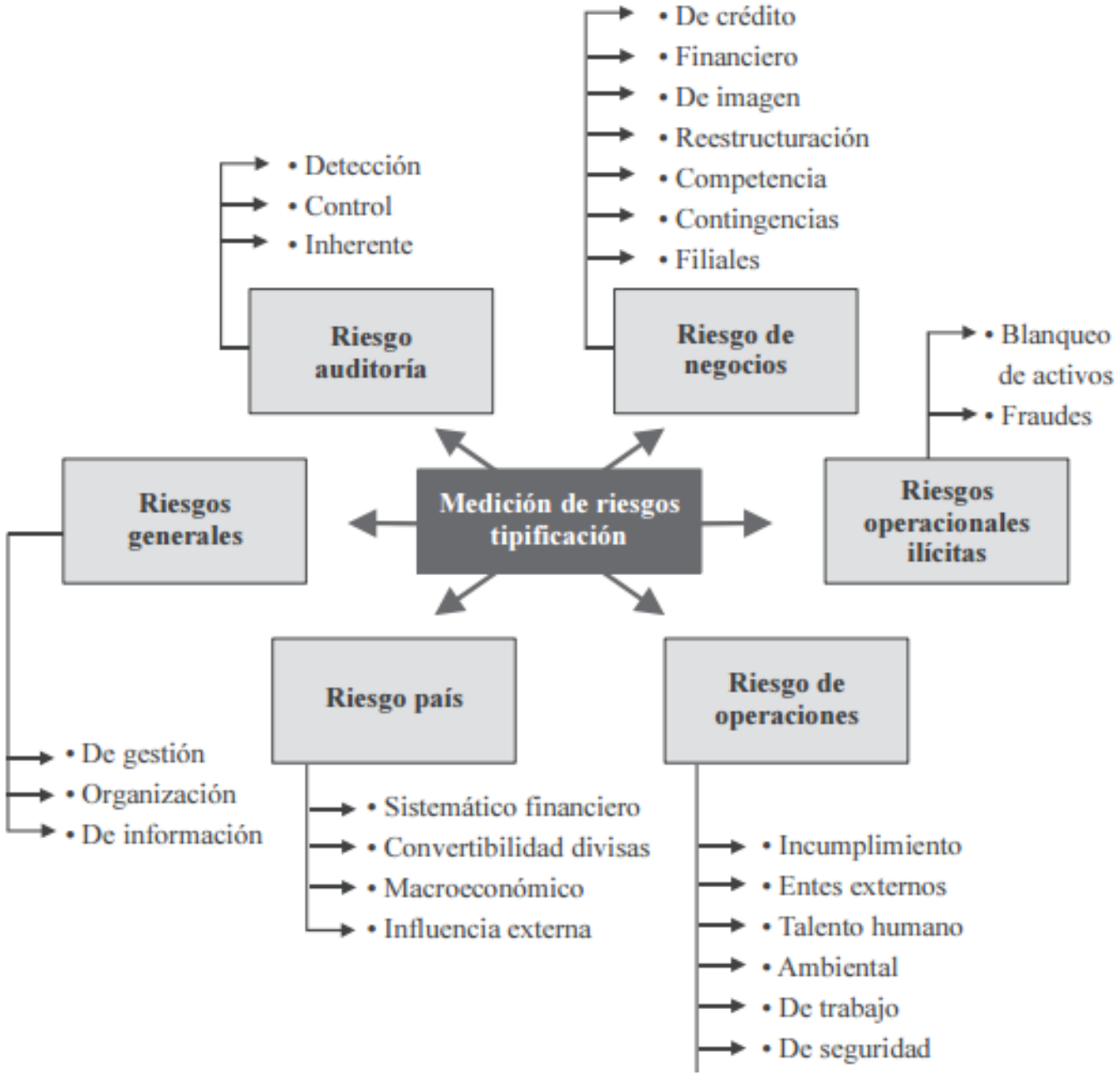
Por ejemplo, “riesgos de mercado”, “riesgo país”, “riesgo operativo”, los cuales afectan interna o externamente a la empresa dentro de las llamadas amenazas y oportunidades que se enfrentan o les favorecen.”

# Gestión de riesgo empresarial

La Gestión de Riesgo Empresarial (ERM) es un componente fundamental del gobierno corporativo. La Dirección es la responsable de establecer y operar el enfoque de gestión de riesgo en nombre del Consejo de Administración. La gestión de riesgos para toda la empresa aporta muchos beneficios como resultado de su enfoque coherente, estructurado y coordinado.

# Gestión de riesgo empresarial

Es responsabilidad de la Administración que los riesgos se abordan adecuadamente y la gestión de riesgo empresarial (ERM) es la mejor manera de hacerlo.


• De crédito
• Financiero
• De imagen
• Reestructuración
• Competencia
• Contingencias
• Filiales
• Detección
• Control
• Inherente
Riesgo auditoría
Riesgo de negocios
• Blanqueo de activos
• Fraudes
Riesgos generales
Medición de riesgos tipificación
Riesgos operacionales ilícitas
Riesgo país
Riesgo de operaciones
• De gestión
• Organización
• De información
• Sistemático financiero
• Convertibilidad divisas
• Macroeconómico
• Influencia externa
• Incumplimiento
• Entes externos
• Talento humano
• Ambiental
• De trabajo
• De seguridad

# Planificación

"Todos los trabajos que proyecte el auditor se deben establecer con planes basados en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna, dichos planes deberán ser consistentes con las metas de la organización, y estarán basados en una evaluación de riesgos, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección."

# LA AUDITORÍA INTERNA COMO ELEMENTO DEL CONTROL

- La auditoría interna examina y evalúa los procesos de planeación, organización y dirección para determinar si existe una garantía razonable de que se logren las metas y objetivos, dichas evaluaciones en conjunto, proporcionan información para evaluar el sistema integral de control.

# LA AUDITORÍA INTERNA COMO ELEMENTO DEL CONTROL

*Disponer de un proceso de gestión de riesgos efectivo facilita la identificación de controles clave relacionados con los riesgos inherentes importantes. Gestión de Riesgo Empresarial (Enterprise Risk Managment), por sus siglas en inglés) es un término de uso común.*

# LA AUDITORÍA INTERNA COMO ELEMENTO DEL CONTROL

El rol principal de la Auditoría Interna con respecto al ERM debe ser brindar aseguramiento a la Dirección y al Consejo de Administración en cuanto a la eficacia de la gestión de riesgo.

Si la Auditoría Interna no asume ninguna función directa en la gestión de riesgos, entonces de manera independiente y objetiva puede realizar cualquier actividad de aseguramiento o consultoría.

# LA AUDITORÍA INTERNA COMO ELEMENTO DEL CONTROL

La auditoria interna es un proceso mediante el cual una organización obtiene seguridad de que la exposición al riesgo que enfrenta, es entendida y manejada apropiadamente dentro de contextos dinámicos cambiantes.

# LA AUDITORÍA INTERNA COMO ELEMENTO DEL CONTROL

*El Committee of Sponsoring Organizations (COSO) of the Treadway Commission define el ERM como: "un proceso efectuado por el Consejo, la alta dirección y restante personal de una entidad, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar acontecimientos potenciales que puedan afectar a la entidad, gestionar sus riesgos dentro de su apetito de riesgo y proporcionar una seguridad razonable sobre el logro de los objetivos de la entidad".*

# Conceptos básicos de la Administración de Riesgos Corporativos.

- Proceso continuo que fluye por toda la entidad.
- Es realizado por su personal en todos los niveles de la organización.
- Se aplica en el establecimiento de la estrategia. En toda la entidad, cada nivel, cada unidad.
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad.
- Es capaz de proporcionar seguridad razonable al Consejo de Administración y a la Dirección de la entidad.
- Orientada al logro de objetivos.

# Beneficios del COSO ERM

- COSO proporciona un marco integral del control interno y herramientas de valuación para evaluar el sistema de control
- Alinea el apetito de riesgo con la estrategia corporativa
- Proporciona respuestas integradas a los múltiples riesgos
- Mejora el nivel de las respuestas al riesgo
- Reduce la posibilidad de sorpresas y pérdidas
- Identifica y administra los riesgos a nivel corporativo
- Prepara a la empresa para tomar ventaja de las oportunidades
- Ayuda a mejorar el uso del capital disponible

# COMPONENTES DE LA ADMÒN. DE RIEGOS CORP. MODELO COSO

## COMPONENTES DE LA ADMÒN. DE RIEGOS CORP. MODELO COSO

Este cubo está representado por:

- Cuatro categorías de objetivos.
- Ocho componentes, y
- La entidad y sus unidades.

# COMPONENTES DE LA ADMÒN. DE RIEGOS CORP. MODELO COSO

- **Categorías de Objetivos**:
  1. Estratégicos
  2. Operativos
  3. De reporte, y
  4. Cumplimiento.

# COMPONENTES DE LA ADMÒN. DE RIEGOS CORP. MODELO COSO

- **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

# COMPONENTES DE LA ADMÒN. DE RIEGOS CORP. MODELO COSO

- **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.

# ELEMENTOS DEL COSO ERM:

- **Los elementos son los siguientes**:
  1. Ambiente Interno (De control y de trabajo).
  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 Y DE TRABAJO

- 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.

# Ambiente de Control y Trabajo

- **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 Alta 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)
- Rol supervisorio de la junta directiva en la gestión integral de riesgo
- La integridad y los valores éticos
- Una estructura de gestión integral de riesgos: Sistemas de delegación de autoridad, roles y responsabilidades y líneas de reporte
- Estándares de recursos humanos: habilidad y competencia de los empleados

# Componente COSO-ERM: Ambiente de Control

Ejemplo

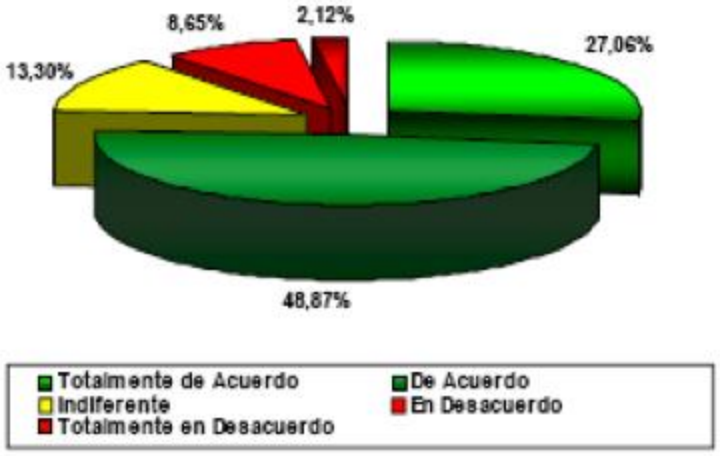
## Filosofía de Gestión de Riesgo

### 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

| Código del Color | Indicador | Rango de la Media Aritmética | Categoría de Respuesta | Puntación |
|---|---|---|---|---|
| Azul | Fuerte | Mayor de 1,66 | Sí, en todo momento | +2 |
| Verde | Bueno | 0,67 a 1,66 | Sí, con algunas excepciones | +1 |
| Amarillo | Precaución | 0,33 a 0,66 | Desconozco la respuesta | 0 |
| Rojo | Revisión sugerida | Menos de 0,33 | No, en todo momento / No, con algunas excepciones | -2 , -1 |

| 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

# Establecimiento de Objetivos

- **Estratégicos:**

  Se refieren a lo que se aspira alcanzar. Sea “misión”, “visión”, o finalidad.

# Establecimiento de Objetivos

- OPERATIVOS:
  - 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.

# Establecimiento de Objetivos

- OBJETIVOS DE REPORTE:
  - Relativos a la confiabilidad de reportes. Incluyen reportes internos y externos y deben involucrar la información financiera y no financiera.

# Establecimiento de Objetivos

- 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.

# Identificacion de Eventos - Riesgos

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 | | | | ✓ |

# Tipos de Riesgos

## Operacionales

- Sistemas operativos
- Expectativas no reales
- Aptitud errónea/gente
- Ejecución
- Procesos de ventas
- Errores
- Cultura errónea
- Pérdida de buenos clientes
- Pérdida de empleados de calidad
- Satisfacción del cliente
- Desarrollo de productos
- Comunicaciones pobres
- Cumplimiento
- Interrupción del negocio
- Falla en Productos/Servicios
- Entorno
- Salud y Seguridad
- Capacidad productiva
- Vacío en el desempeño
- Cíclico (cycle time)
- Obsolescencia

## Estratégicos

- Oportunidad
- Falta de oferta de productos
- Desgaste del mercado
- Conflicto de conducta
- Presupuesto y Planeación
- Reportes Financieros
- Impuestos
- Reportes sobre Reglamentos

## Financieros

- Tasas de Interés
- Moneda
- Volatilidad en los precios
- Flujo de Efectivo
- Inventario Ineficiente
- Costo de Oportunidad
- Incumplimiento de Crédito

## Azarosos

- Daños a Propiedades/Personas
- Errores y omisiones
- Robo/Fraude
- Seguridad
- Siniestro (por ejemplo, auto)

# Identificación de Eventos

- **FACTORES EXTERNOS**.
  - Económicos
  - Medioambientales
  - Políticos
  - Sociales
  - Tecnológicos

# Identificación de Eventos

- **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.

# Identificación de Eventos

- **FACTORES INTERNOS**.
  - Infraestructura
  - Personal
  - Procesos
  - Tecnología

# Identificación de Eventos

- **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.

# RIESGOS DE NEGOCIOS

**Fiscales**
- Pago de impuestos
- Cumplimiento fechas
- Pagos incorrectos

**Estratégicos**
- Estrategias y Objetivos
- Planes de negocio
- Liderazgo y Competitividad

**Laboral**
- Clima Organizacional
- Contingencias laborales
- RRHH competente

**Producción**
- Reprocesos
- Desperdicios / Mermas
- Tiempos muertos

**Producto Marketing**
- Posicionamiento
- Cartera
- Obsolescencia

**Imagen**
- Imagen ante la sociedad
- Cambios de marca
- Impacto en el mercado

## ENTIDAD

**Clientes**
- Fidelidad del cliente
- Cartera moros
- Retención

**Finanzas**
- Cash flow
- Inversiones
- Resultados financieros
- Fiabilidad de la contabilidad

**Sistemas de Información**
- Fiabilidad de la información
- Seguridad e Integridad de la Info
- Vulnerabilidad del sistema

**Compras**
- Inventarios JIT
- Economías de Escala
- Sobre stocks de inventarios

**Logística**
- Costos
- Productividad
- Trazabilidad
- Planificación y programación
- Inventarios obsoletos
- Costos de mantenimiento de inventarios

**Control interno**
- Fraudes
- Políticas y proced.
- Controles débiles

# 4. EVALUACIÓN DEL RIESGO

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

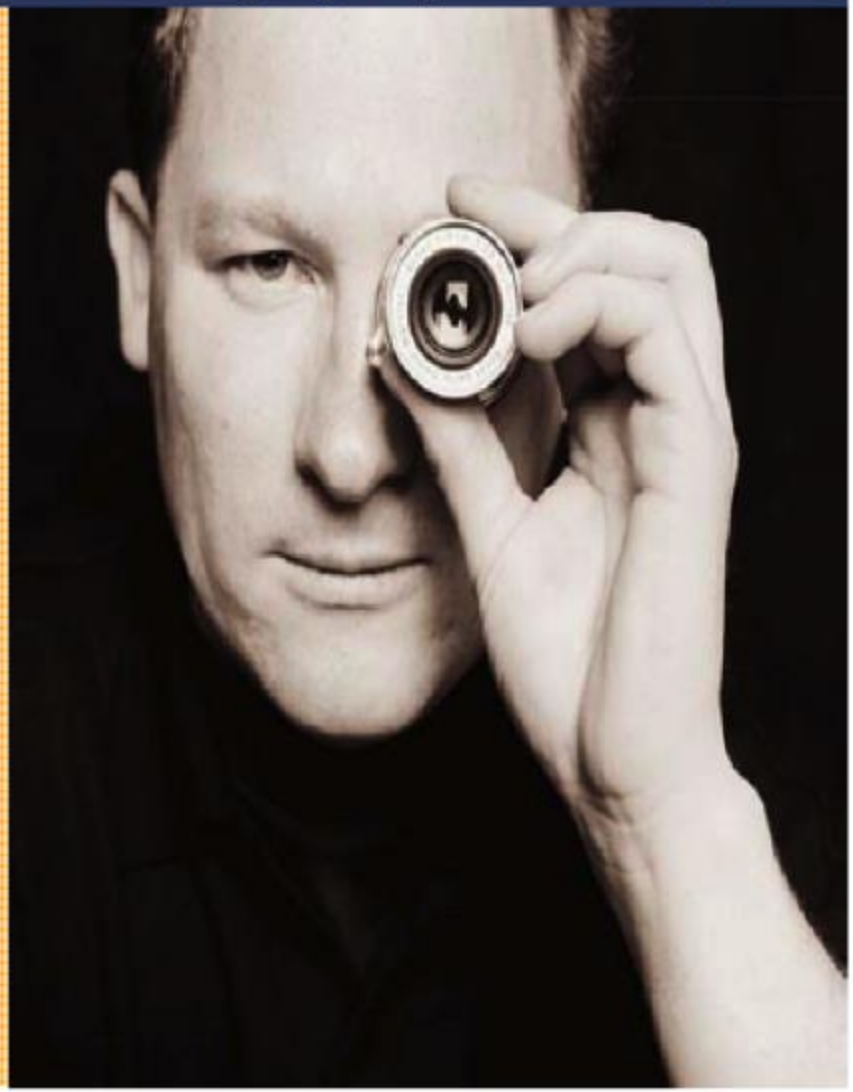
- **Riesgo inherente**: al que se enfrenta en ausencia de acciones de la dirección para modificar su probabilidad.
- **Riesgo residual**: es el que permanece después de que la dirección desarrolle sus respuestas a los riesgos.

# 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**

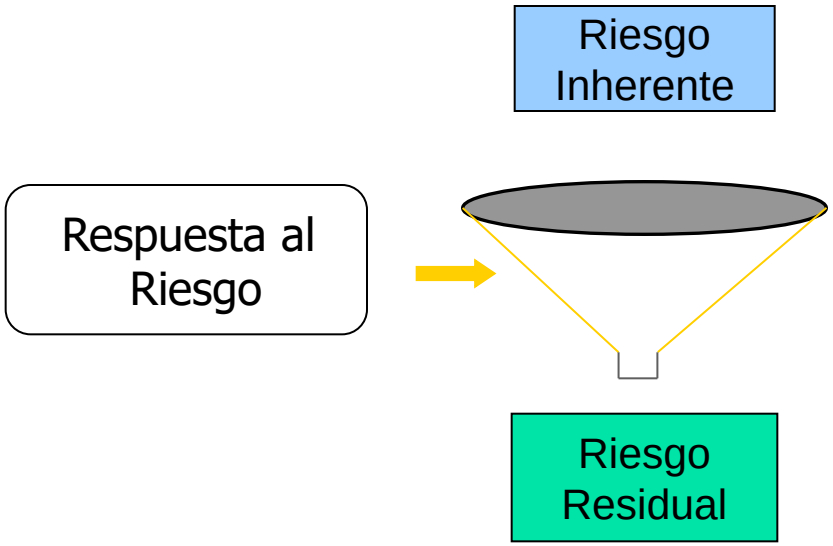
- La gerencia reconoce que la incertidumbre existe, lo cual se traduce en no poder conocer con exactitud cuándo y dónde un evento pudiera ocurrir, así como tampoco sus consecuencias financieras

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



# Evaluación del Riesgo

**Riesgo = Probabilidad X Impacto X Valor del Activo - Controles**




Riesgo Inherente: riesgo para la entidad en ausencia de cualquier acción realizada por la administración para alterar la probabilidad o el impacto.

Riesgo Residual: riesgo remanente después de la acción realizada por la administración para alterar su probabilidad o impacto.

# Evaluación del Riesgo

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

# Evaluación del Riesgo

| Impacto | | |
|---|---|---|
| **1** | Mínimo | |
| **2** | Bajo | |
| **3** | Moderado | |
| **4** | Severo | |
| **5** | Catastrófico | |

| Probabilidad | | |
|---|---|---|
| **1** | Baja | |
| **2** | Menor | |
| **3** | Media | |
| **4** | Mayor | |
| **5** | Alta | |

# Evaluación del Riesgo

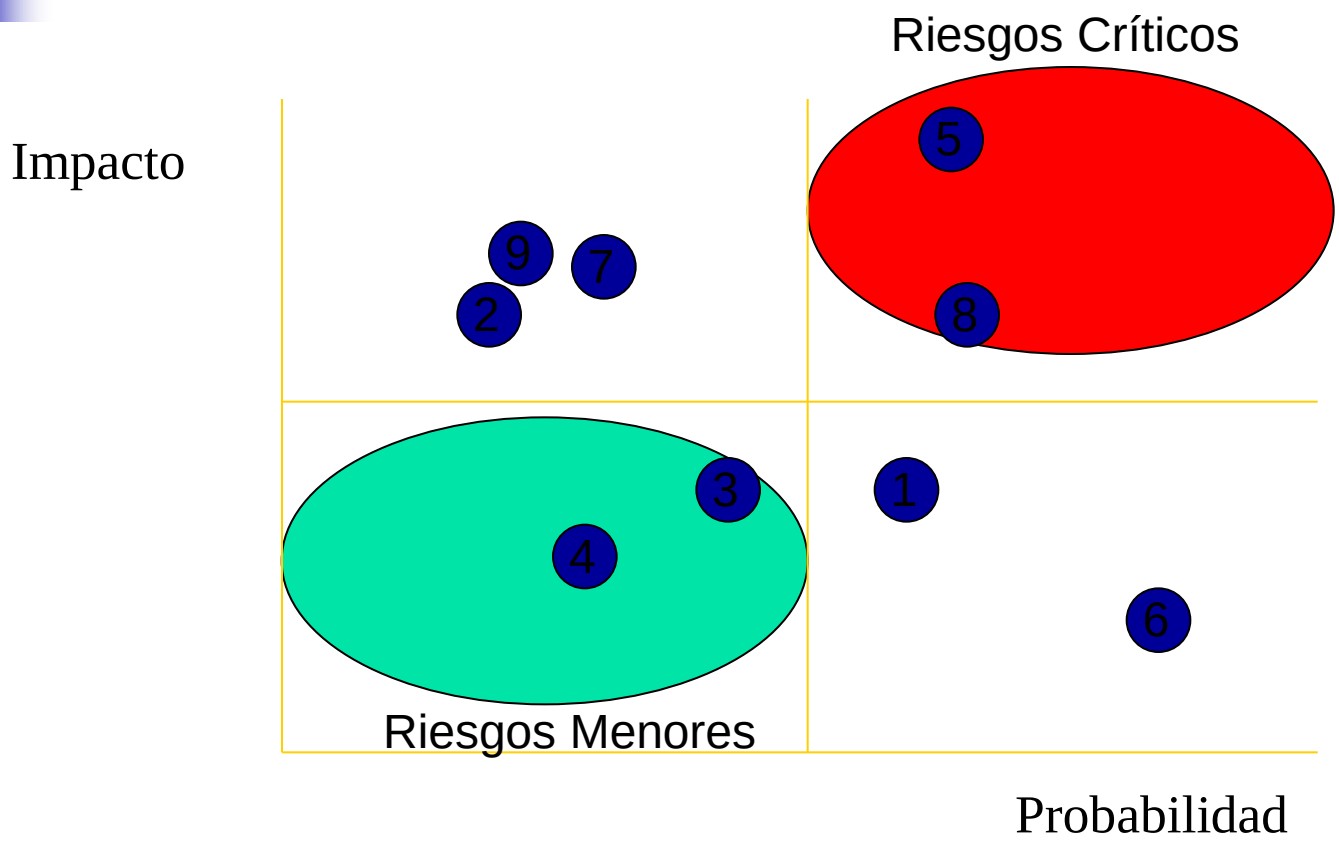
| Riesgos | Area Territorial | Impacto | Probabilidad | Score |
|---|---|---|---|---|
| Nomina | Capital | 4 | 3 | 12 |
| Nomina | Norte | 5 | 2 | 10 |
| Nomina | Sur | 2 | 3 | 6 |
| Nomina | Este | 3 | 2 | 6 |
| Compras | Capital | 5 | 3 | 15 |
| Compras | Norte | 5 | 2 | 10 |
| Compras | Sur | 2 | 3 | 6 |
| Compras | Este | 2 | 2 | 4 |
| Capacitacion | Capital | 1 | 3 | 3 |
| Capacitacion | Norte | 1 | 2 | 2 |
| Capacitacion | Sur | 3 | 3 | 9 |
| Capacitacion | Este | 5 | 2 | 10 |

Numeros mayores indican mayor intensidad

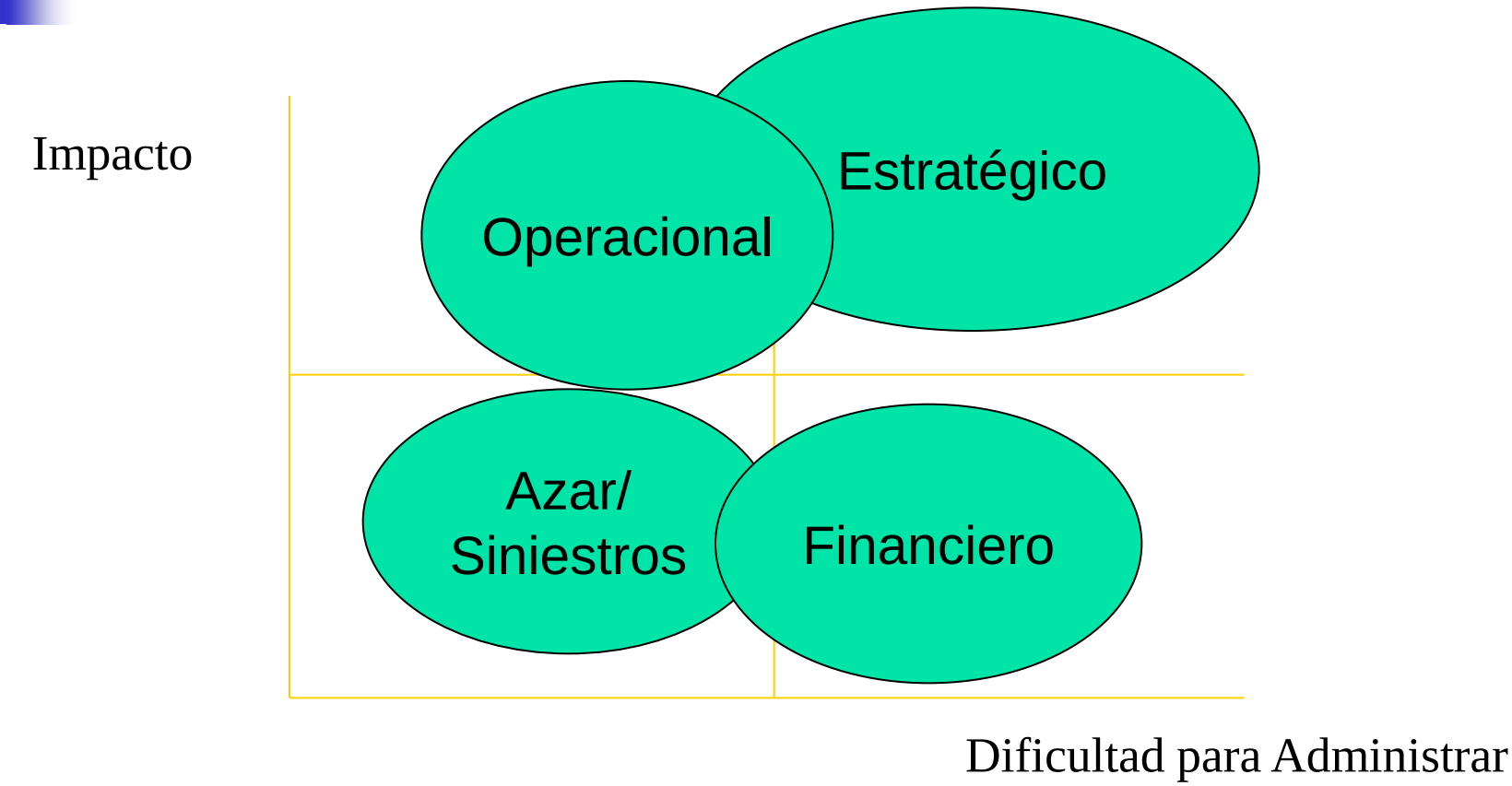
Imprescindible definir valores y medidas claramente

| | Total Score |
|---|---|
| **Capital** | 30 |
| **Norte** | 22 |
| **Sur** | 21 |
| **Este** | 20 |

# Mapa de Riesgos



# Evaluación del Riesgo



# MATRIZ DE RIESGOS
## PROCESO DE COMPRAS


### Resumen por Clasificación de Riesgo:

| Estratégico | Operación | Información / Financiero | Cumplimiento |
|---|---|---|---|
| 1, 2, 3 , 25 | 17, 18, 19 | 24, 21 | 20, 21, 24 |
| 4 | 6, 14, 22, 26 | 7, 10, | 9, 13, 23 |
| | | | |

# 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

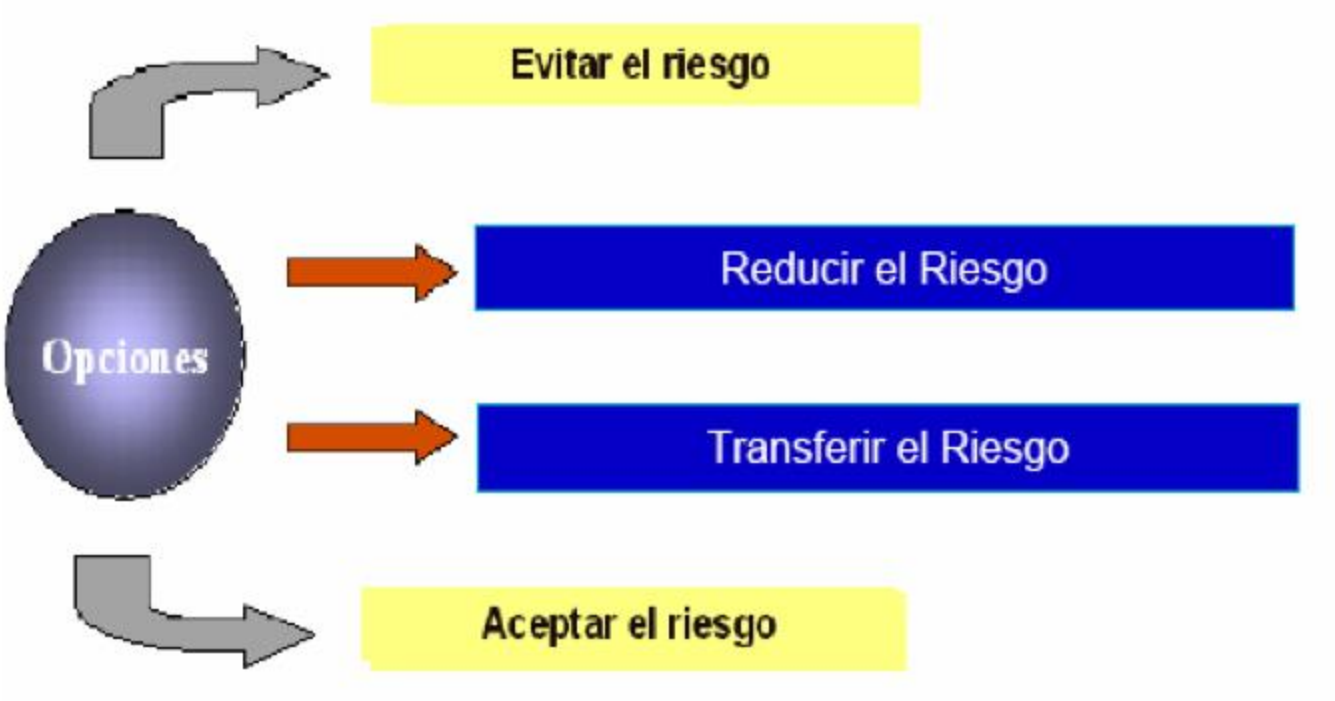
# Respuesta a los Riesgos

- 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
  - Reducción
  - Compartir
  - 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).

# Actividades de Control

- 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<br>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<br>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<br>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:

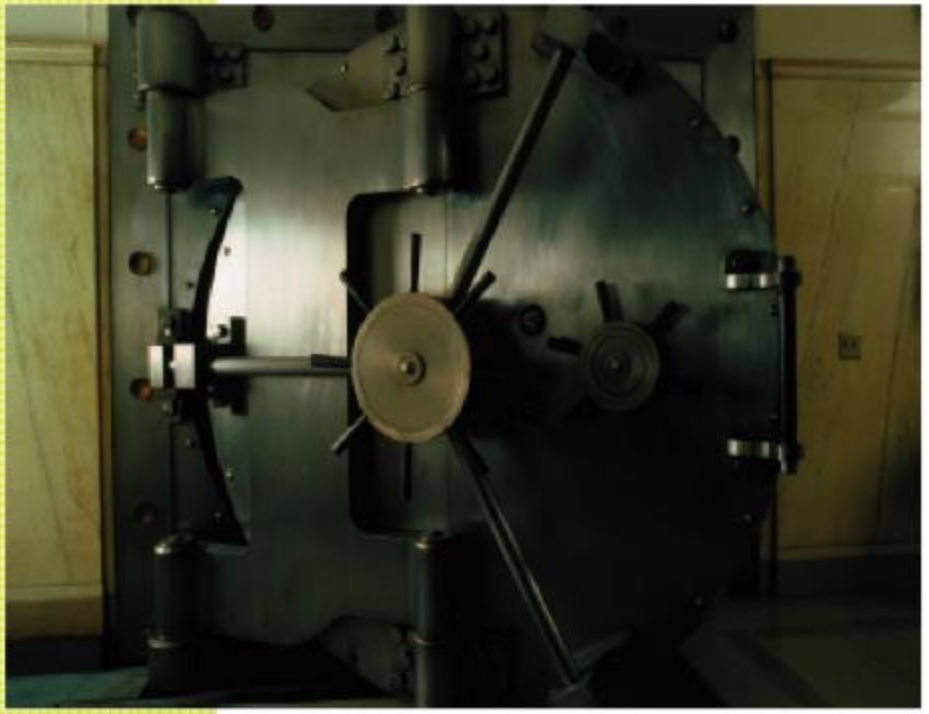
| | |
|---|---|
| Controles preventivos | Diseñados para evitar riesgos, errores o incidentes antes de su ocurrencia |
| Controles detectivos | Diseñados para detectar de forma rápida riesgos, errores o incidentes |
| Controles correctivos | Diseñados para remediar o reducir daños como consecuencia de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

# Componente COSO-ERM: Actividades de Control

**Políticas y procedimientos que ayudan, a la gerencia, a asegurar que las respuestas a los riesgos son ejecutadas de forma apropiada y oportuna**

- 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.

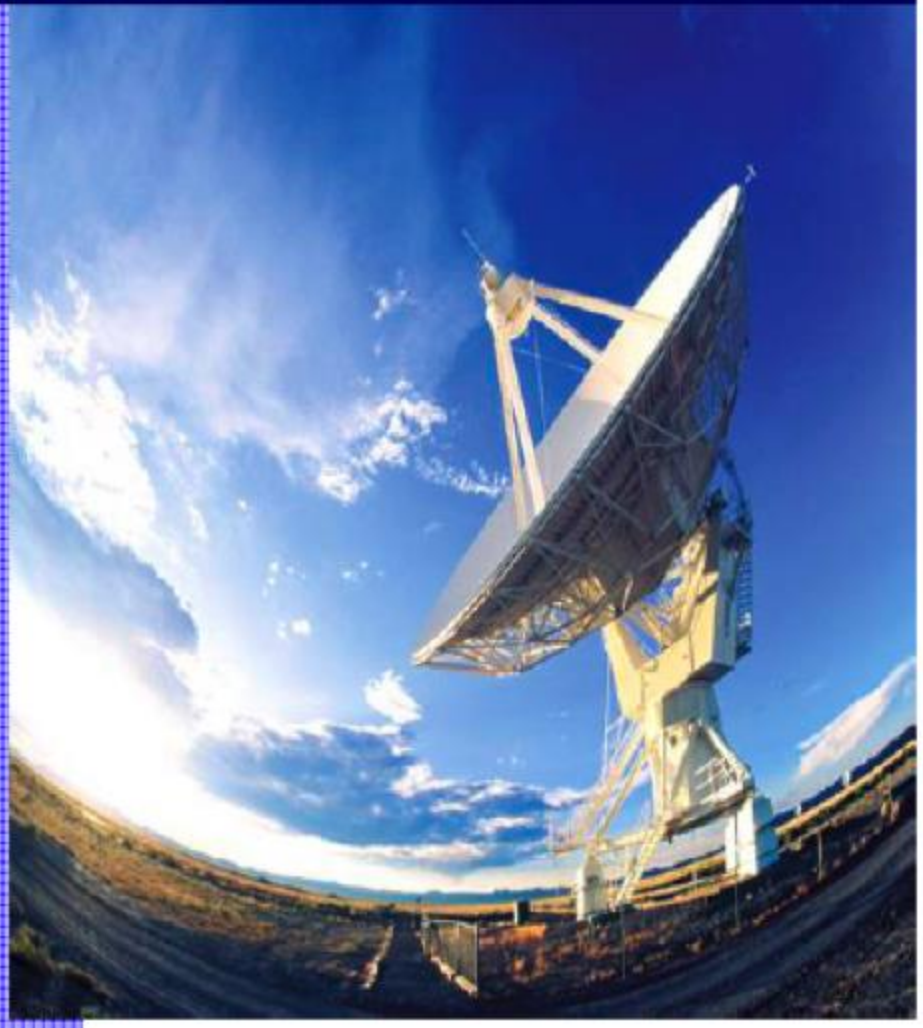
# Información y Comunicación

- 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

**La información relevante, debe ser identificada, capturada, procesada y comunicada en la oportunidad y forma adecuada**

- Los sistemas de información deben apoyar la toma de decisiones y la gestión de riesgo (ERM)
- La gerencia debe enviar un mensaje al personal resaltando su responsabilidad ante el ERM
- El personal debe entender su rol en el ERM así como su contribución individual en relación al trabajo de otros



# 8. SUPERVISIÓN (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.

# Supervisión (Monitoreo)

- 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

# Supervisión (Monitoreo)

- 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.

# Papeles y Responsabilidades

Matriz de Responsabilidades

| | A NIVEL COMPAÑÍA | | | | | UNIDADES OPERATIVAS | | |
|---|---|---|---|---|---|---|---|---|
| Elemento de Control Interno | Director Ejecutivo | Director Operativo | Director Financiero | Contralor | Otros Gerentes | Director de Unidad | Director Financiero de Unidad | Otros Gerentes |
| Pensamiento Estratégico | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ |
| Planeación Interna | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Establecimiento de Metas | ✓ | ✓ | ✓ | | | ✓ | | |
| Marco de Competencia | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Mantener el Alma de las Habilidades | ✓ | ✓ | | | | ✓ | | |
| Soluciones con Innovaciones | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ |
| Aceptación de Riesgo | ✓ | ✓ | ✓ | | | ✓ | ✓ | |
| Procesos y Metodologías | | | | ✓ | ✓ | | ✓ | ✓ |
| Incentivos | ✓ | ✓ | ✓ | | | ✓ | ✓ | |
| Mejora Continua | | | ✓ | | | | | |
| Desarrollo de las Personas | | ✓ | ✓ | | ✓ | | | |
| Valor para el Accionista | ✓ | | ✓ | | | ✓ | ✓ | |
| Información y Análisis | | | ✓ | ✓ | ✓ | | | |
| Orientación de Resultados | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Planeación Exitosa | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# Papeles y Responsabilidades

| 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

# NUEVOS ROLES

- ASEGURAMIENTO
- CONSULTORIA
- AYUDA AL LOGRO DE OBJETIVOS
- CREAR VALOR
- EVALUAR Y MEJORAR EFECTIVIDAD
  - CONTROL
  - RIESGO
  - GOBIERNO CORPORATIVO

# Independencia de la Auditoría Interna Norma 1100

- **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 - ORGANIGRAMA

EMPRESA LA CHABELA, S. A.