Auditoría de la Organización de las TI

AUDITORÍA INFORMÁTICA | IF-8200

Riesgos y Control a nivel de TI

1. CONCEPTOS RELACIONADOS CON RIESGOS
2. ADMINISTRACIÓN DE RIESGOS
3. CONCEPTOS RELACIONADOS CON CONTROL

Riesgos

Concepto de Riesgos

- Falta de Certeza sobre el acontecimiento de una pérdida
- Posibilidad de sufrir una pérdida
- Incertidumbre de que ocurra una pérdida económica
- Conjunto de circunstancias que representen la posibilidad de pérdida

Riesgos

Definición práctica de riesgo:

“Amenaza que una organización no pueda alcanzar sus objetivos”.

Riesgos

Consecuencia	• Resultados tangibles del riesgo sobre las decisiones, eventos o procesos de negocios.
Exposición	• Susceptibilidad hacia una pérdida, o una percepción de una amenaza sobre un proceso, **usualmente cuantificado en términos monetarios**
Amenaza	• Es una combinación del riesgo, la consecuencia de ese riesgo y la posibilidad de que un evento negativo se materialice.
Medición	• Métrica de identificar el grado de impacto u ocurrencia de un riesgo (normalmente se define en ALTO, MEDIO, BAJO)

Riesgos
Clasificación de los Riesgos

RIESGOS CORPORATIVOS

RIESGOS DE LOS PROCESOS

- **TECNOLÓGICOS**
- **AMBIENTALES**
- **DE IMAGEN**
- **ECONÓMICOS**
- **DE PERSONAS**
- **OPERACIONALES**
- **DE DIRECCIONALIDAD**

Riesgos

Tipos de Riesgo: **Económicos | Financieros**

Crédito

Liquidez

Tasa de Interés

Mercado

Sistémico: riesgo sistémico es el riesgo común para todo el mercado entero. Puede ser interpretado como "inestabilidad del sistema financiero, potencialmente catastrófico, causado por eventos idiosincráticos o condiciones en los intermediarios financieros".

Riesgos

Tipos de Riesgo: **Operacionales**

Problemas de seguridad

Error en la operación de los Sistemas de TI

Mal uso del producto o servicio por parte de los clientes

Riesgos

Riesgos Tecnológicos

Ocurren cuando la Tecnología de Información usada en la Institución, no está operando según lo planeado, no existe una integridad y confiabilidad de los datos e información. Además, que no se estén soportando apropiadamente los procesos críticos.

Riesgos

Tipos de Riesgo: **Tecnológicos**

- Pérdida de Información
- Acceso no Autorizado y Suplantación
- Error u omisión en el procedimiento
- Pérdida de Confidencialidad
- Fraude o Hurto
- Interrupción de Operaciones por negación del servicio en uno de los componentes.

Riesgos

Tipos de Riesgo: **Reputación | Imagen**

- Producto en mal estado
- Exposición a robos
- Errores en la información

Riesgos
Tipos de Riesgo: **Legal**

Atrasos en Obligaciones Obrero – Patronales.

Atrasos en pago de impuestos.

Administración del Riesgo

Proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales.

Administración del Riesgo

Se reconoce como una parte integral de las buenas prácticas administrativas.

Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejoramiento.

Si no es posible integrar la administración del riesgo en toda la organización, podría ser posible aplicarla exitosamente en departamentos, procesos o proyectos individuales.

Administración de Riesgos
Beneficios para la Organización

Facilita el logro de los objetivos de la organización

Hace a la organización más segura y consciente de sus riesgos

Mejoramiento continuo del Sistema de Control Interno

Optimiza la asignación de recursos

Aprovechamiento de oportunidades de negocio

Fortalece la cultura de Autocontrol.

Mayor estabilidad ante los cambios del entorno

Administración de Riesgos
Beneficios para la Auditoría

Soporta el logro de los objetivos de la Auditoría

Estandarización en el método de trabajo

Integración del concepto de control en las políticas organizacionales

Mayor efectividad en la planeación general de Auditoría

Evaluaciones enfocadas en Riegos

Mayor cobertura de la administración de Riesgos.

Auditorías más efectivas y con mayor valor agregado.

Administración de Riesgos

1. **Establecer Marco General**
   - Establecer el Contexto estratégico
   - Establecer el Contexto Organizacional
   - Identificar Objetos Críticos
2. **Identificar Riesgos**
   - Establecer un marco específico de administración de riesgos
   - Desarrollar criterios de evaluación de riesgos
   - Identificar la estructura
   - Identificar riesgos
   - Identificar causas

Administración de Riesgos

3. **Análisis de Riesgos**
   - Valorar el riesgo inherente
   - Determinar controles existentes
   - Identificar nivel de exposición
4. **Evaluar y Priorizar Riesgos**
   - Comparar contra criterios y definir prioridades de riesgo

Administración de Riesgos

5. **Tratamiento del Riesgo**
   - Identificar opciones de tratamiento
   - Evaluar opciones de tratamiento
   - Preparar planes de tratamiento
   - Implementar plan de tratamiento
6. **Monitoreo y Revisión**

Administración de Riesgos

Tópicos de interés para identificar riesgos

Deben impactar los objetivos

No deben ser causales o factores

Son amenazas posibles, aunque no hayan ocurrido

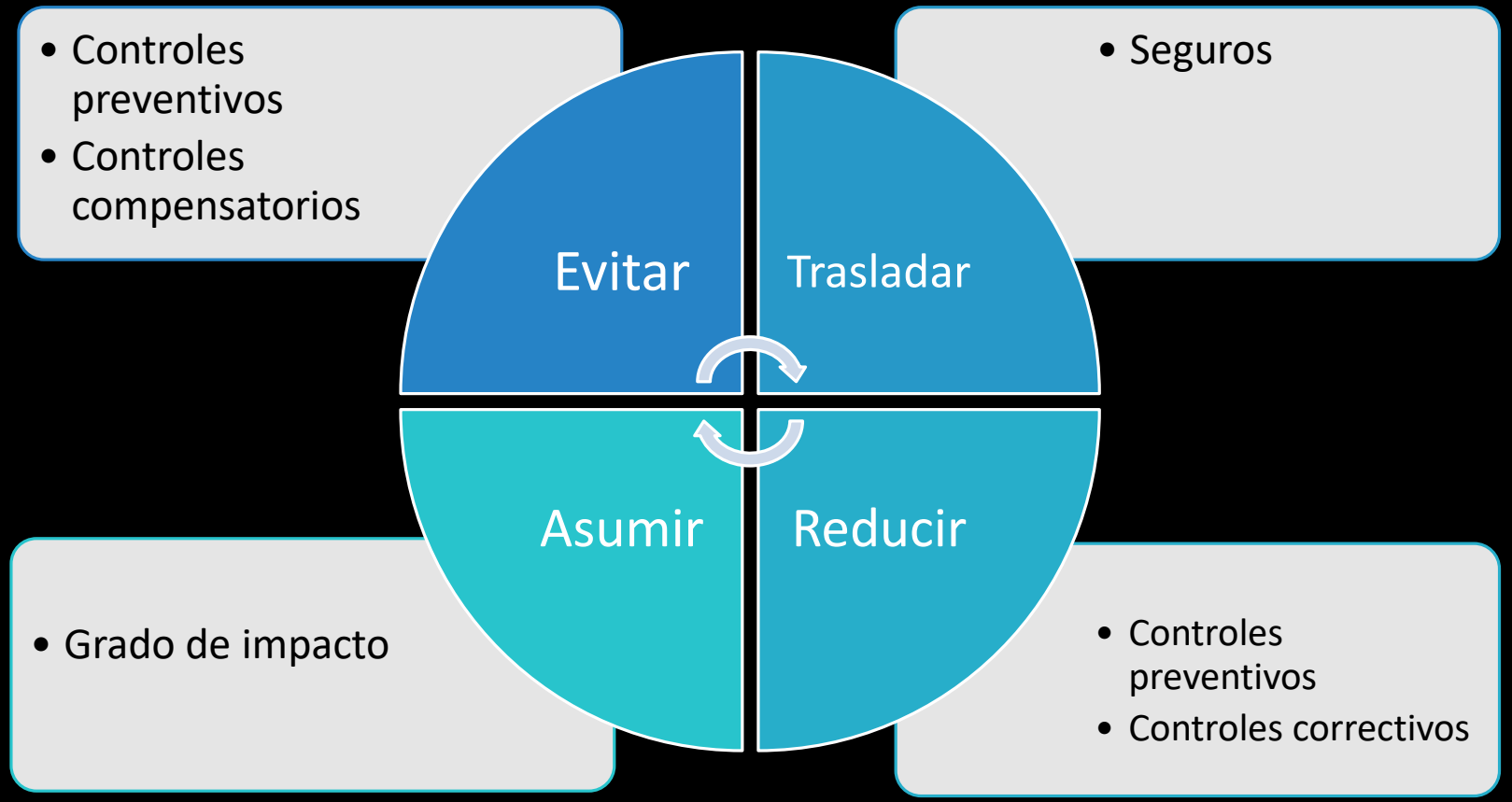
Se trata de identificar, no de valorar

Deben ser de alto nivel y holísticos

Considere el interno y el entorno

Revise interrelaciones entre elementos

Control
Control: respuestas de la Administración entre el Riesgo



Control

Objetivos de Control

- Los objetivos de control deben determinar la existencia de controles adecuados para proteger los recursos comprometidos en el sistema, a efecto de reducir al máximo su grado de exposición al riesgo y que este último no se materialice. Los objetivos básicos son:
  - Protección de los activos de la empresa
  - Obtención de información veraz, confiable y oportuna.
  - Promoción de la eficiencia en la operación del negocio
  - Que la ejecución de las operaciones se adhiera a las políticas

Control

Objetivos de Control Definidos

- En busca de un ambiente con nivel de control y seguridad adecuados, se establecieron los siguientes objetivos de control:
  - Confidencialidad
  - Disponibilidad
  - Integridad
    - Objetivo de Totalidad
    - Objetivo de existencia
    - Objetivo de exactitud

Control

Objetivos de Control Definidos

- *Confidencialidad*
  - La protección de la información en la infraestructura de TI instalada, para que personas no autorizadas no puedan accesarla.

Control

Objetivos de Control Definidos

- *Disponibilidad*
  - La garantía de que la infraestructura de TI instalada, está accesible para los usuarios autorizados cuando estos lo necesiten.

Control

Objetivos de Control Definidos

- *Integridad*
  - La protección de los datos que el sistema almacena contra cambios intencionales o accidentales no autorizados.
  - Para efectos de esta auditoría hemos dividido este objetivo en tres:
    - Objetivo de Totalidad
    - Objetivo de existencia
    - Objetivo de exactitud

Control

Objetivos de Control Definidos

- *Integridad*
  - *Objetivo de Totalidad*
    - **A nivel de entrada**. Todos los datos son ingresados
    - **A nivel de proceso**. Todos los datos son procesados y solo una vez.
    - **A nivel de salidas**. La información que brindas las salidas del sistema está completa

Control

Objetivos de Control Definidos

- *Integridad*
  - *Objetivo de existencia*
    - **A nivel de entrada**. La entrada de datos es validada, autorizada y registrada solo una vez.
    - **A nivel de salida**. La salida está disponible para soportar los registros de la corporación.

Control

Objetivos de Control Definidos

- *Integridad*
  - *Objetivo de exactitud*
    - **A nivel de entrada**. Los datos son exactos en todos sus detalles esenciales.
    - **A nivel de proceso**. Los datos son procesados con exactitud.
    - **A nivel de salida**. Los reportes (o consultas) que el sistema genera son exactos y confiables.

Control
Controles institucionales y de TI

El sistema institucional de Controles Internos impacta a TI en estos niveles

- Al nivel de Alta Gerencia:
  - Se fijan los objetivos institucionales, se establecen políticas y se toman decisiones de cómo aplicar y administrar los recursos institucionales para ejecutar la estrategia de la compañía
- Al nivel de procesos Institucionales
  - Se aplican controles para actividades específicas de la institución. La mayoría de los procesos específicos de la institución. La mayoría de los procesos institucionales están automatizados e integrados con los sistemas aplicativos de TI, dando como resultado que muchos de los controles a este nivel estén incorporados en dichos aplicativos.

Control
Controles institucionales y de TI

Controles generales de TI

- Para soportar los procesos institucionales, TI proporciona servicios, por lo de forma compartida, por varios procesos institucionales, así como procesos operacionales y de desarrollo de TI que se proporcionan a toda la institución, y mucha de la infraestructura de TI provee un servicio común (es decir, redes, bases de datos, sistemas operativos y almacenamiento)

Control
Controles generales y controles de aplicación

Es decir, los **controles generales** son aquellos que están incrustados en los procesos y servicios de TI

- Ejemplos: Desarrollo de sistemas, Administración de cambios, Seguridad, Operación del computador

Los controles incluidos en las aplicaciones del proceso operativo se conocen por lo general como **controles de aplicación**.

- Ejemplos: Integridad (completitud), precisión, validez, autorización, segregación de funciones.