AUDITORÍA

Preparado por Dr(c) Jorge Morris A
Ing. Civil Industrial
Ing. Informático (E)

Versión 2.1 2012
Parte II

AUDITORÍA

CONTENIDOS

- **Introducción**
- **Objetivos de la Auditoría Computacional**
- **Tipos de Auditorías**
- **Controles Básicos, Disciplinarios y de Integridad**
- **Seguridad e Instalación de Sistemas de Información**
- **Normativas de Seguridad de Sistemas de Información**

AUDITORÍA INFORMÁTICA

El uso de computadores para procesar la información en los últimos años, la evolución tecnológica, el riesgo asociado al uso de la información, y los objetivos que la organización se propone, determinan que deben existir *Sistemas de Control,* adecuados para asegurar la integridad de dicha información.

AUDITORÍA INFORMÁTICA

Control

- **El control es la fase del proceso administrativo que debe mantener la actividad organizacional dentro de los límites permisibles, de acuerdo con las expectativas.**
- **El control organizacional está irremediablemente relacionado con la planeación.**
- **Los planes son el marco de referencia dentro del cual funciona el proceso de control.**
- **MECANISMO o PROCEDIMIENTO que EVITA o PREVIENE un RIESGO.**

AUDITORÍA INFORMÁTICA

Control Interno

En la organización, la administración es responsable por Establecer, Diseñar y Mantener Controles y Procedimientos Internos, adecuados para alcanzar los objetivos organizacionales.

AUDITORÍA INFORMÁTICA

Control Interno

El control interno surge por la necesidad de evaluar y satisfacer la eficiencia, eficacia, razonabilidad, oportunidad y confiabilidad en la protección, protección y seguridad en los bienes de una empresa, así como ayudar a controlar el desarrollo de sus operaciones, actividades y resultados financieros que se esperaban obtener en el desempeño de las funciones y operaciones de toda la empresa

AUDITORÍA INFORMÁTICA

Tipos de Control

Controles Preventivos (Proactivos)

Aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Ejemplos:

- **Letrero "No fumar" para proteger las instalaciones**
- **Sistemas de claves de acceso**

AUDITORÍA INFORMÁTICA

Tipos de Control

Controles Detectivos (Reactivos)

Aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos.

Son importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Ejemplos:

- **Archivos y procesos que sirvan como pistas de auditoría**
- **Procedimientos de validación**

AUDITORÍA INFORMÁTICA

Tipos de Control

Controles Correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si, una actividad altamente propensa a errores.

AUDITORÍA INFORMÁTICA

Objetivos del Control

- **Establecer estándares,**
- **Medir su cumplimiento,**
- **Evaluar el alcance real de los planes y programas, comparado con lo realmente alcanzado.**
- **Proteger y salvaguardar de los bienes y activos de la empresa.**
- **Planificar y evaluar correctamente el cumplimiento de las funciones, actividades y operaciones de la empresa.**

AUDITORÍA INFORMÁTICA

Componentes del Control

Definir los componentes fundamentales del control, permite identificar la forma de utilizar el control interno en las empresas y así poder aplicar ese conocimiento al control interno en sistemas, y más concretamente a las aplicaciones especificas de auditoría de Sistemas Computacionales.

- **Una característica medible y controlable para la que se conocen estándares.**
- **Un medio (instrumento censor) para medir las características.**
- **Un medio para comparar los resultados reales con los estándares y evaluar las diferencias y,**
- **Un medio para efectuar cambios en el sistema a fin de ajustarlos a las necesidades**

AUDITORÍA INFORMÁTICA

Características del Control

El control en las empresas será efectivo, cuando éste sea:

- ***Oportuno***

Característica esencial del control, debido a que es la presentación a tiempo de los resultados obtenidos con su aplicación; es importante evaluar dichos resultados en el momento que se requieran, no antes porque se desconocerían sus verdaderos alcances, ni después puesto que ya no servirían para nada.

AUDITORÍA INFORMÁTICA

Características del Control

El control en las empresas será efectivo, cuando éste sea:

- ***Cuantificable***

Para que verdaderamente se puedan comparar los resultados alcanzados contra los esperados, es necesario que sean medibles en unidades representativas de algún valor numérico, para así poder cuantificar, porcentual o numéricamente lo que se haya alcanzado.

AUDITORÍA INFORMÁTICA

Características del Control

El control en las empresas será efectivo, cuando éste sea:

- **Calificable**

  Así como los valores de comparación deben ser numéricos para su cuantificación, en las Auditoría de Sistemas Computacionales, se dan casos de evaluaciones que no necesariamente deben ser de tipo numérico, ya que, en algunos casos específicos, en su lugar se pueden sustituir estas unidades de valor, por conceptos de calidad o por medidas de cualidad.

AUDITORÍA INFORMÁTICA

Características del Control

El control en las empresas será efectivo, cuando éste sea:

- **Calificable**
  - **Estos valores son de carácter subjetivo, pero pueden ser aplicados para evaluar el cumplimiento, relativos a la calidad.**
  - **Siempre y cuando en la evaluación sean utilizados de manera uniforme tanto para planear como para medir los resultados.**

AUDITORÍA INFORMÁTICA

Características del Control

El control en las empresas será efectivo, cuando éste sea:

- ***Confiable***

Para que el control sea útil, debe señalar resultados correctos sin desviaciones ni alteraciones y sin errores de ningún tipo, a fin de que se pueda confiar en que dichos resultados siempre son valorados con los mismos parámetros.

AUDITORÍA INFORMÁTICA

Características del Control

El control en las empresas será efectivo, cuando éste sea:

Estandarizado y normalizados en cuanto a la evaluación

Al medir los resultados alcanzados, estos deberán ser comparados de acuerdo con los estándares y normas previamente establecidos, a fin de contemplar las mismas unidades para planear y controlar - se logra una estandarización que permite valorar adecuadamente los alcances obtenidos. -

AUDITORÍA INFORMÁTICA

Riesgos y controles
en procesos operativos
MANUALES

Riesgos y controles
en procesos operativos
AUTOMATIZADOS

AUDITORÍA INFORMÁTICA

Riesgos y controles en procesos operativos MANUALES

Riesgos y controles en procesos operativos AUTOMATIZADOS

Revisión periódica de procedimientos de controles establecidos

Detección de riesgos

Seguimiento de errores o irregularidades

AUDITORÍA INFORMÁTICA

Riesgos

“La incertidumbre que ocurra un evento que podría tener un impacto en el logro de los objetivos”.

AUDITORÍA INFORMÁTICA

Riesgos

Los riesgos cuando se materializan, se denominan errores, irregularidades u omisiones, los cuales pueden generar una pérdida de tipo:

- **Monetaria,**
- **En la imagen de la empresa, o**
- **Incumplimiento de Normativas Externas.**

AUDITORÍA INFORMÁTICA

Riesgos

Riesgo = Impacto * Probabilidad

Impacto : Efecto o consecuencia cuando el riesgo se materializa

Probabilidad: Posibilidad que un evento dado ocurra.

Ejercicio

Identifique los posibles riesgos que se puedan deducir de el siguiente enunciado. Clasificarlos como del proyecto. Ordene por orden de probabilidad e impacto los riesgos. Genere una gráfica de interrelación entre los riesgos, y establezca protocolos de actuación en caso de suceder.

- **Una empresa de menos de 3 años en el sector de las TIC decide abordar un proyecto de firmas digitales para la administración.**
- **Decide hacer el desarrollo con Java.**
- **Acaba de salir la versión 1.5 de la máquina virtual.**
- **La empresa tiene 5 expertos en Java, 3 Medios y 8 sin conocimientos de Java.**
- **La planificación se ha hecho para 6 meses con un esfuerzo de400 t-d.**
- **El jefe de desarrollo ha decidido usar un nuevo compilador, Eclipse por su versatilidad en entornos multiplataforma que es nuevo para el equipo de desarrollo.**

AUDITORÍA INFORMÁTICA

Riesgos

Riesgo Inherente

- Aquellos riesgos propios de la materia y/o componentes de ésta.

- Se entiende que una materia por su naturaleza tiene riesgos que surgen por diversas fuentes, como los errores, irregularidades o fallas que pudieran ser importantes en forma individual o en conjunto con otros riesgos.

AUDITORÍA INFORMÁTICA

Riesgos

Riesgo Inherente

- Los riesgos inherentes a la materia pueden tener o no controles elaborados por la dirección para mitigar su probabilidad o su impacto.

- Los riesgos inherentes a la materia bajo análisis pueden ser relativos al entorno, ambiente interno, procesos, información, etc

AUDITORÍA INFORMÁTICA

Riesgos

Riesgo Inherente

- **Riesgo de Crédito**
- **Riesgo Financiero**
- **Riesgo Operacional**
- **Riesgo de Tecnología de la Información**
- **Riesgo Calidad de Servicio y transparencia de la Información**

AUDITORÍA INFORMÁTICA

- **Riesgo Financiero:**

  Ocurrencia de un imprevisto por variaciones o cambios en la economía local o internacional que podría afectar los descalces de caja o posiciones asumidas por inversiones y su liquidez, como asimismo los descalces globales de activos.

- **Riesgo Operacional:**

  Se define como el riesgo de pérdida debido a la inadecuación o fallas en los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos (fraudes, daños activos materiales, fallas en procesos, etc.). Incluye riesgos legales y normativos.

AUDITORÍA INFORMÁTICA

- **Riesgo de Crédito:**

  Exposición a una pérdida real o el costo de oportunidad como consecuencia del incumplimiento de pago de una persona natural o jurídica.

AUDITORÍA INFORMÁTICA

Matriz de Valoración de Riesgo

- La Matriz de Evaluación de Riesgos constituye un mecanismo útil que apoya a la organización a estar dentro de las políticas, procedimientos y objetivos estratégicos relacionados con los riesgos.

- Interpretar en términos de niveles de riesgos aceptables las actividades de la organización.

AUDITORÍA INFORMÁTICA

Uso de la Matriz de Valoración de Riesgo

- Evaluar acciones operativas y de mantenimiento.
- Investigar y clasificar accidentes.
- Seleccionar procedimientos y estándares.
- Generar decisiones en Ingeniería
- Otros.

AUDITORÍA INFORMÁTICA

Uso de la Matriz de Valoración de Riesgo

La Matriz de Evaluación de Riesgos es una herramienta para la evaluación cualitativa de los riesgos y facilita la clasificación de las amenazas a la salud, seguridad, medio ambiente, relación con clientes, bienes e imagen de la Empresa

AUDITORÍA INFORMÁTICA

Uso de la Matriz de Valoración de Riesgo

- Los ejes de la matriz según la definición de riesgo corresponden a las consecuencias y a la probabilidad.
- Para determinar el nivel de las consecuencias se utiliza una escala de "0" a "5“.
- Para evaluar la probabilidad se utiliza una escala de “A” a “E”, basándose en la experiencia o evidencia histórica en que las consecuencias identificadas se han materializado dentro de la Empresa, o el área.

AUDITORÍA INFORMÁTICA

Uso de la Matriz de Valoración de Riesgo

- Representa la probabilidad de que se desencadenen las consecuencias potenciales o reales estimadas, según el caso.
- El cruce de las dos escalas determina la evaluación y clasificación cualitativa del riesgo.
- Para este caso de la RAM, estimar la probabilidad y las consecuencias no es una ciencia exacta.

AUDITORÍA INFORMÁTICA

Uso de la Matriz de Valoración de Riesgo

- La estimación de la consecuencia se basa en la respuesta a “qué ocurrió” o “qué pudo o podrá ocurrir”.
- Mientras que la estimación de la probabilidad se basa en información histórica respecto de casos ocurridos anteriormente en similares condiciones, sabiendo que las circunstancias nunca son exactamente las mismas.

AUDITORÍA INFORMÁTICA

Ejemplos de Aplicación

Área o Tema	*Ejemplo*
Diseño	**Estudio de Factibilidad, Evaluaciones de impactos, Selección de Estándares y/o Normas, Aplicación de control de Cambio**
Planeación	**De Mantenimiento, De producción, Procedimiento de Adquisición Priorización de acciones de mantenimiento y/o inversiones**
Construcción, mantenimiento, Instalación	**Ausencias, Selección de códigos y prácticas de diseño e ingeniería Selección en guías de salud ocupacional y seguridad en construcción, Inspección basada en el Riesgo**
Puesta en Marcha	**Sistemas de Permisos, Procedimientos de Inicio y/o partida**
Producción	**Sistemas de Permisos, Procedimiento de Cambio, Procedimientos de Movimientos**
Procesos	**Financieros, Vulnerabilidad, Políticas de personal, Producción Requerimientos**

AUDITORÍA INFORMÁTICA

Elementos considerados en el diseño de una Matriz de Riesgo

En base de los objetivos estratégicos y plan de negocios, la “administración de riesgos” debe desarrollar un proceso para la “identificación” de las actividades principales y los riesgos a los cuales están expuestas (entendiéndose como riesgo la eventualidad de que una determinada entidad no pueda cumplir con uno o más de los objetivos.

AUDITORÍA INFORMÁTICA

CLASIFICACIÓN DE LOS FACTORES DE RIESGO

FACTORES DE RIESGO FÍSICOS

Son aquellos factores ambientales de naturaleza física que, cuando las personas se exponen a ellos, éstos pueden provocar daños en la salud, según la intensidad y la concentración de los mismos.

AUDITORÍA INFORMÁTICA

ALGUNOS FACTORES DE RIESGO FÍSICOS

FACTOR DE RIESGO FÍSICO	EJEMPLOS DE FUENTE GENERADORA DE PELIGRO	EJEMPLOS DE MEDIDAS DE PREVENCIÓN Y CONTROL
RUIDO	TALADRO DE BANCO SIERRA CIRCULAR MARTILLO	ENCERRAMIENTO, MANTENIMIENTO DE MAQUINARIA. ELEMENTOS DE PROTECCIÓN PERSONAL.
TEMPERATURAS EXTREMA	CALOR FRIO	SISTEMAS DE AIRE ACONDICIONADO, ELEMENTOS DE PROTECCIÓN PERSONAL. MÉTODOS DE REFRACCIÓN DEL CALOR CALEFACCIÓN, ROPA TÉRMICA, CONTROL EN EL TIEMPO DE EXPOSICIÓN, PERIODOS DE ADAPTACIÓN
ILUMINACIÓN DEFICIENTE	LUMINARIAS	DISTRIBUCIÓN ADECUADA DE LAS LÁMPARAS. MANTENIMIENTO DE LUMINARIAS.
ILUMINACIÓN EN EXCESO	LUZ NATURAL, LUMINARIAS	DISTRIBUCIÓN ADECUADA DE LAS LÁMPARAS. PERSIANAS, FILTROS-

AUDITORÍA INFORMÁTICA

CLASIFICACIÓN DE LOS FACTORES DE RIESGO

FACTORES DE RIESGO ERGONÓMICOS

Son todos los objetos, puestos de trabajo, máquinas, mesas y herramientas que por su peso, tamaño, forma o diseño, pueden producir fatiga física o lesiones en músculos o huesos.

AUDITORÍA INFORMÁTICA

ALGUNOS FACTORES DE RIESGO ERGONÓMICOS

FACTOR DE RIESGO ERGONÓMICOS	EJEMPLOS DE FUENTE GENERADORA DE PELIGRO	EJEMPLOS DE MEDIDAS DE PREVENCIÓN Y CONTROL
POSICIÓN DE PIE PROLONGADO	ACTIVIDADES DE VIGILANCIA. OPERACIÓN DE MAQUINARIA.	PAUSAS ACTIVAS, TAPETES ERGONÓMICOS, HIGIENE POSTURAL.
POSICIÓN SENTADO PROLONGADO	LABORES DE OFICINA EN GENERAL	HIGIENE POSTURAL, PAUSAS ACTIVAS, PUESTO DE TRABAJO ERGONÓMETRICO
MOVIMIENTOS REPETITIVOS	DIGITAR. OPERACIÓN DE MAQUINAS EN SERIE.	PAUSAS ACTIVAS, HIGIENE POSTURAL, ORGANIZACIÓN DEL TRABAJO, ASIGNACIÓN DE TAREAS VARIAS.
HIPEREXTENSIÓN	ALCANZAR OBJETOS QUE ESTÁN UBICADOS POR FUERA DEL ALCANCE DE LA MANO	REDISEÑO DEL PUESTO DE TRABAJO

AUDITORÍA INFORMÁTICA

CLASIFICACIÓN DE LOS FACTORES DE RIESGO

FACTORES DE RIESGO PSICOSOCIALES

Se refiere a todos aquellos factores que pueden generar insatisfacción, aburrimiento, estrés o poca disposición para hacer las tareas.

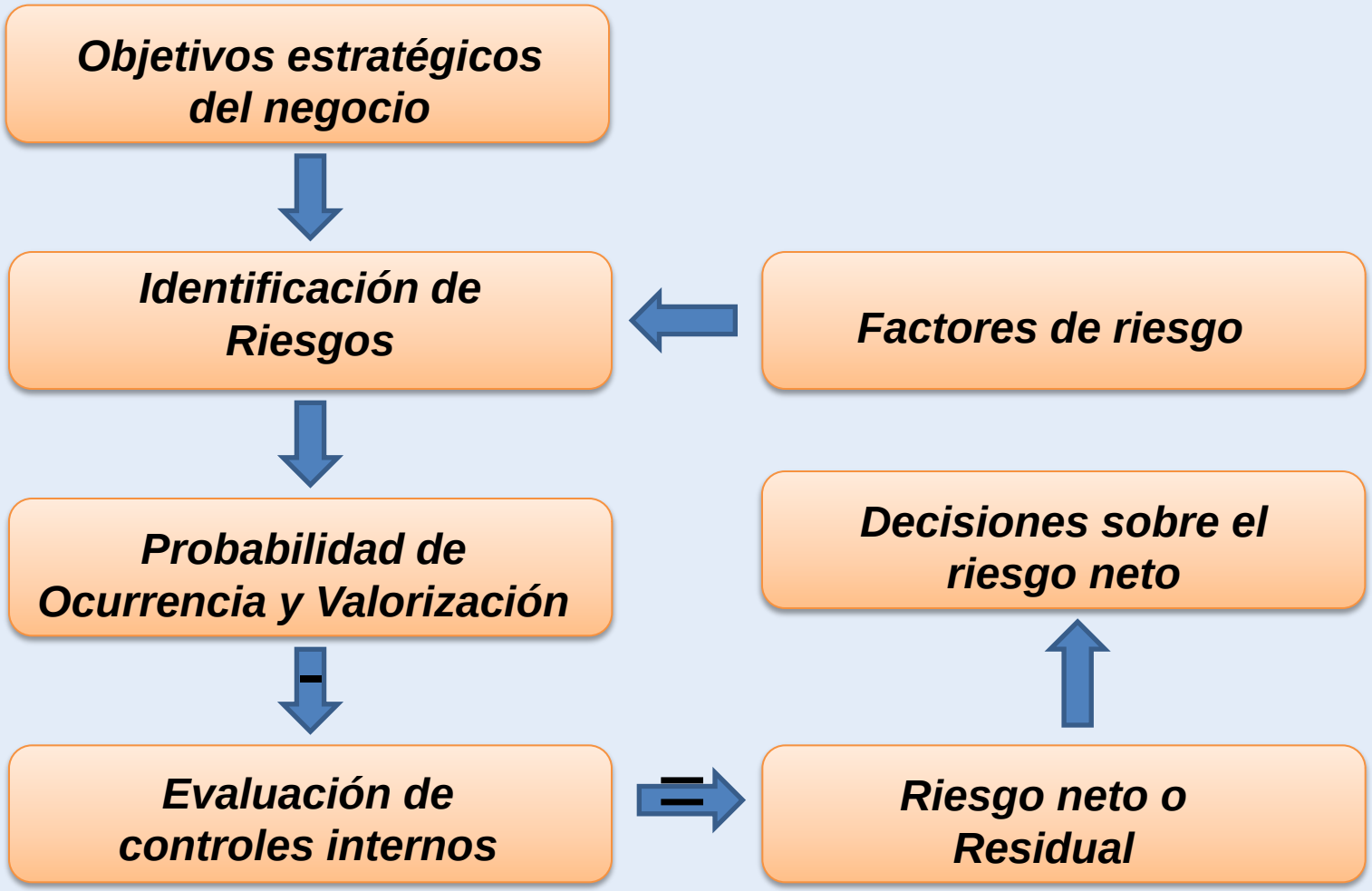
AUDITORÍA INFORMÁTICA

ALGUNOS FACTORES DE RIESGO PSICOSOCIALES

FACTOR DE RIESGO PSICOSOCIALES	EJEMPLOS DE FUENTE GENERADORA DE PELIGRO	EJEMPLOS DE MEDIDAS DE PREVENCIÓN Y CONTROL
CONFLICTOS INTERPERSONALES	DESACUERDO ENTRE COMPAÑEROS DE TRABAJO, PROBLEMAS FAMILIARES	ESTABLECER MEDIOS Y MEDIDAS QUE FAVOREZCAN UNA COMUNICACIÓN ASERTIVA, PROPICIAR EL TRABAJO EN EQUIPO
ALTOS RITMOS DE TRABAJO	ACUMULACIÓN DE TRABAJO	REORGANIZACIÓN DEL TRABAJO, PROPONER MANERAS DIFERENTES DE REALIZAR LAS ACTIVIDADES DIARIAS, IMPLEMENTAR PROGRAMAS PARA EL MANEJO DEL ESTRÉS
SOBRECARGA DE TRABAJO	SUPRESIÓN DE CARGOS, NO REEMPLAZO DE PERSONAS AUSENTES	AUTOMATIZACIÓN DE PROCESOS, REDISEÑO DE LOS PERFILES DE CARGO
CAPACITACIÓN INSUFICIENTE	PERFILES DE CARGO MAL DISEÑADOS	CREAR PLANES DE CAPACITACIÓN, TENER PERSONAS CON LA CAPACITACIÓN Y LOS CONOCIMIENTOS IDÓNEOS PARA LAS TAREAS A DESEMPEÑAR

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo



AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

Objetivos estratégicos del negocio

Identi… R…

Proba… Ocurrencia…

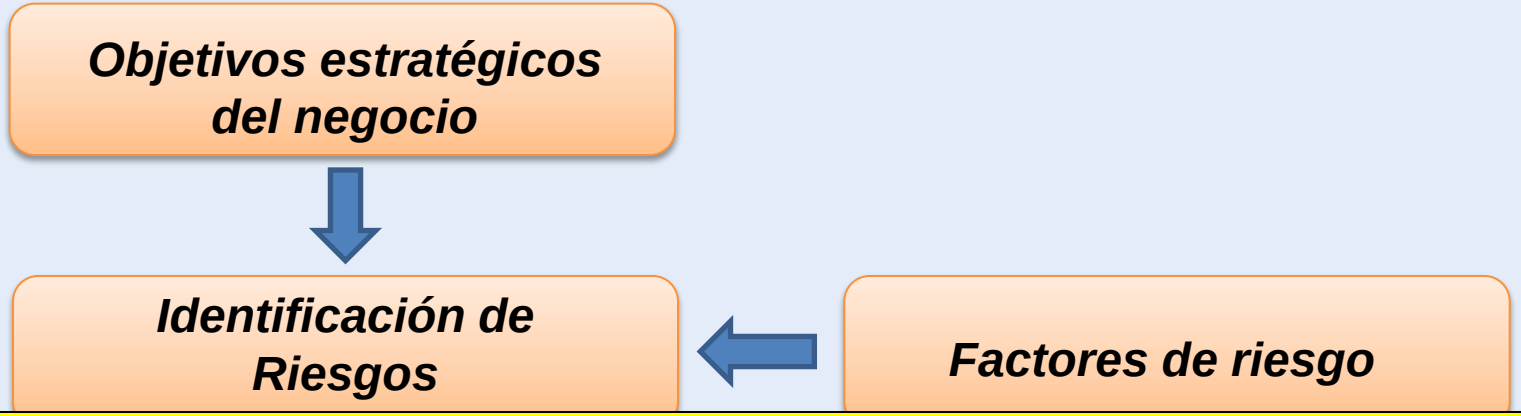
En base a los objetivos estratégicos y plan de negocios, la administración de riesgos debe desarrollar un proceso para la "identificación" de las actividades principales y los riesgos a los cuales están expuestas; entendiéndose como riesgo la eventualidad de que una determinada entidad no pueda cumplir con uno o más de los objetivos.

Evaluación de controles internos

Riesgo neto o Residual

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo



- ***Consecuentemente, una vez establecidas todas las actividades, se deben identificar las fuentes o factores que intervienen en su manifestación y severidad, llamados "factores de riesgo o riesgos inherentes".***

- ***El riesgo inherente es intrínseco a toda actividad, surge de la exposición y la incertidumbre de probables eventos o cambios en las condiciones del negocio o de la economía que puedan impactar una actividad.***

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

- **El riesgo inherente Es aquel riesgo que por su *naturaleza* no se puede separar de la situación donde existe.**
- **Es propio del trabajo a realizar.**
- **Es el riesgo propio de cada empresa de acuerdo a su actividad.**

TIPO DE EMPRESA	PRINCIPALES RIESGOS INHERENTES
Transporte	Choques, colisiones, volcamiento
Metalmecánica	Quemaduras, golpes,
Construcción	Caída distinto nivel, golpes, atrapamiento
Minería	Derrumbes, explosiones, caídas atrapamiento
Servicios	Choque, colisiones, lumbago, caídas
Desarrollo Informático	

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

- *Objetivos estratégicos del negocio*
- *Identificación de Riesgos*
- *Probabilidad de Ocurrencia y Valorización*
- *Evaluación de controles internos*

- ***Los factores o riesgos inherentes pueden no tener el mismo impacto sobre el riesgo agregado, siendo algunos más relevantes que otros, por lo que surge la necesidad de ponderar y priorizar los riesgos primarios.***
- ***Los riesgos inherentes al negocio de las entidades financieras pueden ser clasificados en riesgos crediticios, de mercado y liquidez, operacional, legales y normativos estratégicos.***

AUDITORÍA INFORMÁTICA

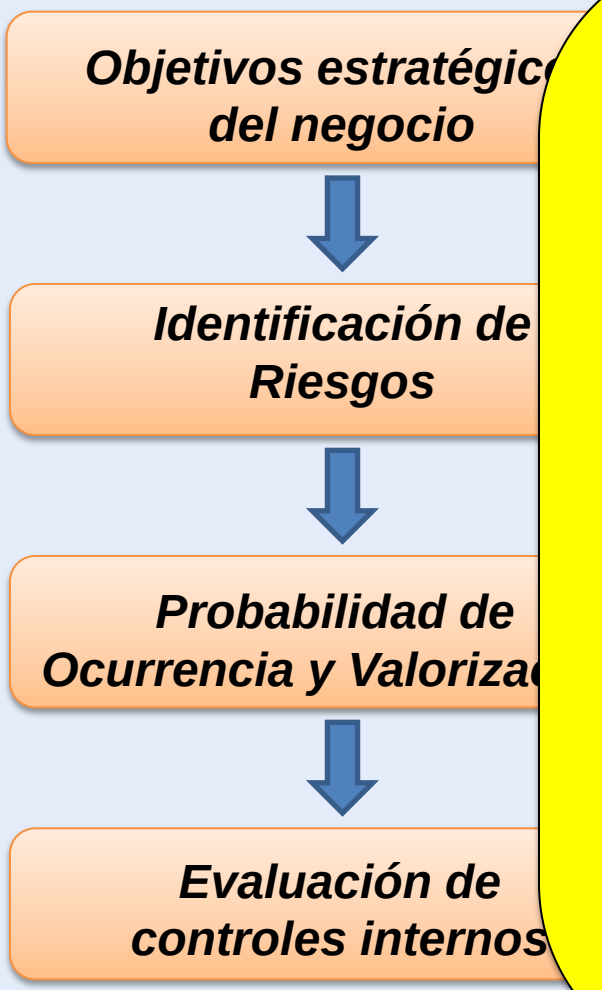
Fases de la elaboración de una Matriz de Riesgo

- ***Objetivos estratégicos del negocio***
- ***Identificación de Riesgos***
- ***Probabilidad de Ocurrencia y Valorización***
- ***Evaluación de controles internos***

- La valorización cualitativa no involucra la cuantificación de parámetros, utiliza escalas descriptivas para evaluar la probabilidad de ocurrencia de cada evento.
- En general este tipo de evaluación se utiliza cuando el riesgo percibido no justifica el tiempo y esfuerzo que requiera un análisis más profundo o cuando no existe información suficiente para la cuantificación de los parámetros.

AUDITORÍA INFORMÁTICA

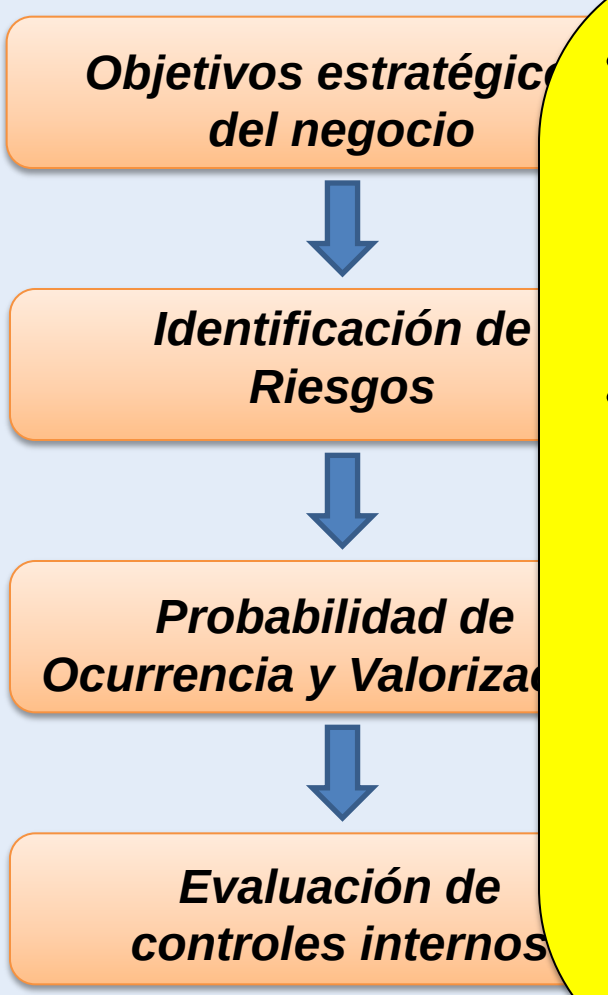
Fases de la elaboración de una Matriz de Riesgo



- En el caso de riesgos que podrían afectar significativamente los resultados, la valorización cualitativa se utiliza como una evaluación inicial para identificar situaciones que ameriten un estudio más profundo.
- La evaluación cuantitativa utiliza valores numéricos o datos estadísticos, en vez de escalas cualitativas, para estimar la probabilidad de ocurrencia de cada evento.

AUDITORÍA INFORMÁTICA

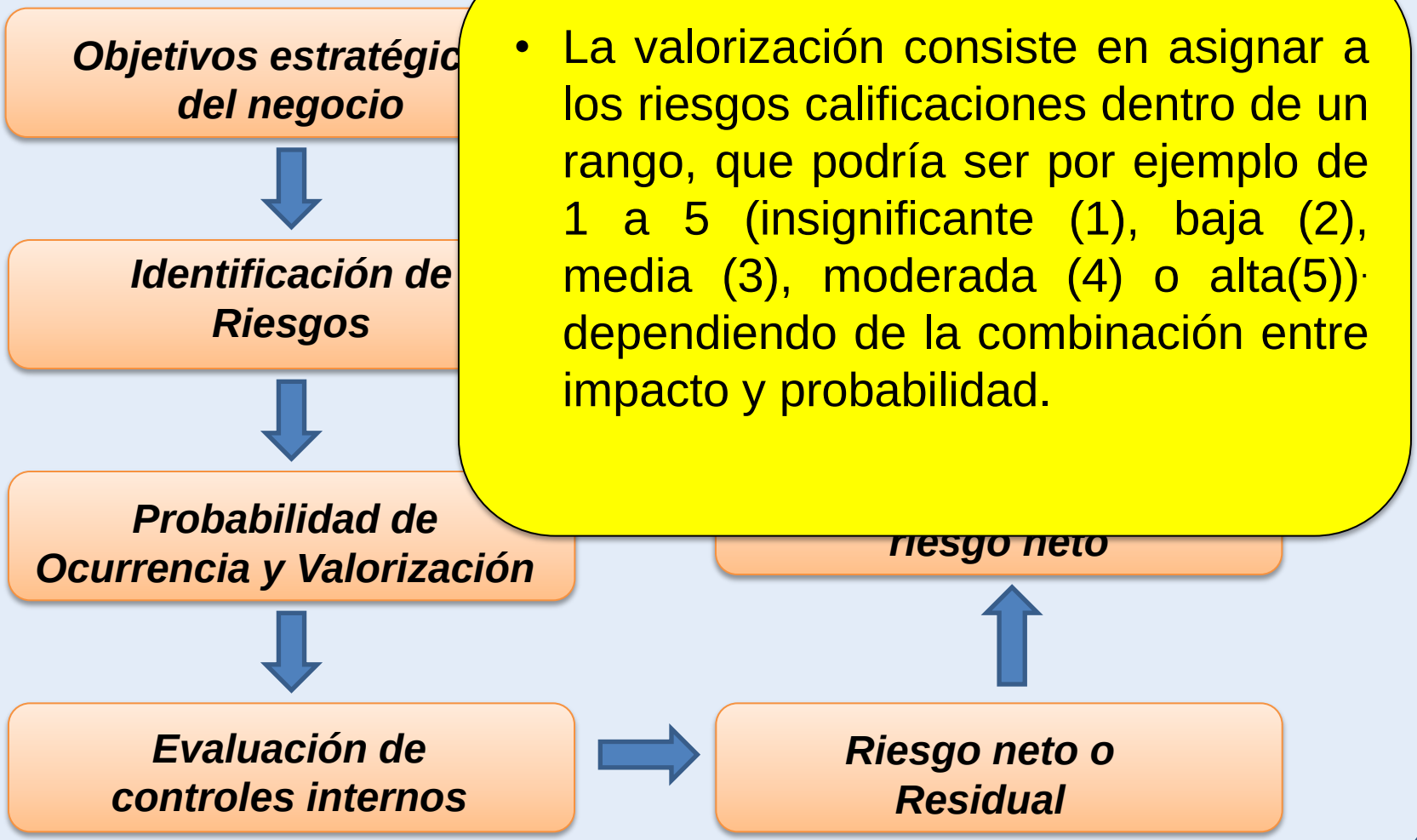
Fases de la elaboración de una Matriz de Riesgo



- Ambas estimaciones, cualitativa y cuantitativa, pueden complementarse en el proceso del trabajo de estimar la probabilidad de riesgo.
- Debe notarse que si bien la valoración de riesgo contenida en una matriz de riesgo es mayormente de tipo cualitativo, también se utiliza un soporte cuantitativo basado en una estimación de eventos ocurridos en el pasado, con lo cual se obtiene una mejor aproximación a la probabilidad de ocurrencia del evento.

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo



- La valorización consiste en asignar a los riesgos calificaciones dentro de un rango, que podría ser por ejemplo de 1 a 5 (insignificante (1), baja (2), media (3), moderada (4) o alta(5)) dependiendo de la combinación entre impacto y probabilidad.

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

Clasificación de Consecuencias

Categoría 1	Categoría 2	……	Categoría n	
				5
				4
				:
				0

Niveles de Gravedad

Los niveles de Gravedad están en una escala de consecuencia 0 a 5.

EVALUACIÓN DE LAS CONSECUENCIAS

La evaluación y clasificación de las consecuencias debe hacerse basándose en lo que podrá o podría haber ocurrido bajo condiciones levemente diferentes (consecuencias potenciales estimadas) o en lo que realmente ocurrió, dependiendo la actividad que se esté evaluando o clasificando, a saber.

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

Clasificación de Consecuencias

Categoría 1	Categoría 2	.....	Categoría n	
				5
				4
				:
				0

Niveles de Gravedad

Los niveles de Gravedad están en una escala de consecuencia 0 a 5.

Situación Hipotética	*Consecuencia Real*	*Consecuencia Potencial*
De una grúa cae una carga a un metro de una persona.	Daño a la carga	Lesión fatal si la persona hubiera estado debajo de la carga
Pérdida de un computador portátil en la empresa.	Daño económico por la reposición del equipo y pérdida de info.	Fuga de información confidencial
Sabotaje a los canales de red de datos.	Pérdida de comunicación para las unidades en la empresa	Pérdidas económicas y retraso en la entrega de productos

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

Ejemplos Valoración de Consecuencias

Falla	*Personas*	*Económicas*	*Imagen*	*Clientes*
Sistema fuera de plazo	Responsabilidad Alta	Entre 5 -100 UTM	Externa	Alto Impacto
Pérdida de Calidad	Responsabilidad Alta	Entre 5 -100 UTM	Interna-Externa	Alto Impacto
Caída de la RED de datos	Baja Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Violación de Claves de Acceso	Baja Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Pérdida de Información	Alta Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Ausencia de Seguridad Perimetral	Baja Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Datos inconsistentes	Alta responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Accesos remotos externos	Mediana Responsabilidad	Entre 5 -100 UTM	Interna-Externa	Mediano Impacto

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

Ejemplos Valoración de Consecuencias

Falla	*Personas*	*Económicas*	*Imagen*	*Clientes*
Sistema fuera de plazo	Responsabilidad Alta	Entre 5 -100 UTM	Externa	Alto Impacto
Pérdida de Calidad	Responsabilidad Alta	Entre 5 -100 UTM	Interna-Externa	Alto Impacto
Caída de la RED de datos	Baja Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Violación de Claves de Acceso	Baja Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Pérdida de Información	Alta Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Ausencia de Seguridad Perimetral	Baja Responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Datos inconsistentes	Alta responsabilidad	Entre 5 -100 UTM	Interna	Ningún Impacto
Accesos remotos externos	Mediana Responsabilidad	Entre 5 -100 UTM	Interna-Externa	Mediano Impacto

Que le falta para que esté correcta??

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

EVALUACIÓN DE LA PROBABILIDAD

El eje horizontal representa la medición de probabilidad de la ocurrencia del evento, con la consecuencia identificada. La escala del eje horizontal se define como (generalmente):

A – No ha ocurrido en la Industria (Sector)
B – Ha ocurrido en la Industria (Sector)
C – Ha ocurrido en nuestra Empresa
D – Sucede varias veces por año en nuestra Empresa
E – Sucede varias veces por año en la Unidad, Departamento, u otro.

"No debe confundirse con la probabilidad de que se produzca el peligro: se trata de la probabilidad de que se produzcan las consecuencias potenciales o reales estimadas, según sea el caso".

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

EVALUACIÓN DE LA PROBABILIDAD

Probabilidad

A	B	C	D	E
No ha ocurrido en la Industria (Sector)	Ha ocurrido en la Industria (Sector)	Ha ocurrido en la Empresa	Sucede varias veces por año en la Empresa	Sucede varias veces por año en la Unidad

A medida que aumenta la gravedad de la consecuencia, proporcionalmente aumenta la probabilidad

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

CLASIFICACIÓN DE LOS RIESGOS

La evaluación y clasificación de los riesgos debe hacerse teniendo en cuenta los siguientes tres elementos:

- **El primero es la categoría de consecuencia con la cual está relacionada la evaluación.**
- **El segundo corresponde a la gravedad de las consecuencias: 0-5.**
- **El tercero corresponde al nivel de probabilidad del suceso: A-E.**

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

CLASIFICACIÓN DE LOS RIESGOS

La intersección de la fila elegida con la columna seleccionada corresponde a la clasificación del riesgo.

Los incidentes pueden tener consecuencias en las cinco categorías, por lo tanto, para una evaluación o clasificación, deben examinarse las categorías definidas.

El riesgo de un incidente se debe clasificar de acuerdo con la categoría de consecuencia que tenga la mayor clasificación, por ejemplo: para un caso en el que se encuentre que el riesgo para personas es 5C, el económico 2C, el de medioambiente 1D, el de clientes 2D e imagen 1C: el riesgo de este incidente será 5C.

AUDITORÍA INFORMÁTICA |

Fases de la elaboración de una Matriz de Riesgo

Consecuencias – Amenazas y Oportunidades

Alto	**Alto impacto financiero en la empresa.** **Impacto significativo en la estrategia de la organización o en la operatividad.** **Preocupación de los interesados significativa. (*«quienes pueden afectar o son afectados por las actividades de una empresa».)***
Medio	**Impacto medio financiero en la empresa.** **Impacto moderado sobre la estrategia de la organización o las actividades operacionales.** **Preocupación de los interesados Moderado.**
Bajo	**Bajo impacto financiero en la empresa.** **Bajo impacto en la estrategia de la organización o en la operatividad.** **Menor preocupación de los interesados.**

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

Consecuencias – Amenazas y Oportunidades

Estimación	*Descripción*	*Indicador*
Alto (Probable)	**Probabilidad de que ocurra cada año o más del 25% de probabilidad de ocurrencia.**	**Potencial de que ocurra varias veces dentro del periodo de tiempo (por ejemplo. – diez años). Ha ocurrido recientemente.**
Medio (Posible)	**Probabilidad de que ocurra en un período de diez de tiempo o menos de un 25% de probabilidad de ocurrencia.**	**Podría ocurrir más de una vez dentro del período de tiempo (por ejemplo.- diez años). Podría ser difícil de controlar debido a algunas influencias externas. ¿Hay antecedentes de que se produzca?**
Bajo (Remoto)	**No es probable que se produzca en un período de diez años o menos, 2% de probabilidad de ocurrencia.**	**No ha ocurrido. Es poco probable que se produzca.**

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

SECUENCIA - CLASIFICACIÓN DE LOS RIESGOS

Para evaluar el riesgo de un caso en particular se debe seguir la siguiente secuencia:

- **Defina la actividad que requiere evaluar o clasificar.**
- **Conforme el equipo que realizará la evaluación del riesgo, con máximo de seis personas de experiencia en el trabajo. Se debe tener en cuenta que evaluar no es para principiantes: *la experiencia del equipo es la clave de una buena evaluación.***
- **Defina si para el caso que se analiza se requiere evaluar las consecuencias reales o potenciales.**
- **Determine el riesgo para las categorías de: Personas, Económicas, Ambiente, Cliente e Imagen dela Empresa. (o Categorías definidas).**

AUDITORÍA INFORMÁTICA

Fases de la elaboración de una Matriz de Riesgo

SECUENCIA - CLASIFICACIÓN DE LOS RIESGOS

- **Estime las consecuencias reales o potenciales, dependiendo del caso que se analiza para la categoría seleccionada. No se requieren datos de precisión, busque consenso de la mayoría del equipo que hace el análisis.**

- **Busque el punto dentro de la matriz correspondiente a la consecuencia y la probabilidad determinadas: esa será la valoración del riesgo.**

  Para su interpretación las letras corresponden a:

  N= Ninguno; L= Bajo; M = Medio; H = Alto y VH = Muy Alto.

- **Repita el proceso para la siguiente categoría hasta que cubra todas las posibles pérdidas : Personas ,Económica, Ambiente, Cliente, Imagen, etc.**

AUDITORÍA INFORMÁTICA

Ejemplo:
Caso: EMPRESA DE SERVICIOS DE CONSULTORÍA EN TI

Actividades Principales	Factores de Riesgos
Desarrollo	Servidor de Aplicaciones fuera de servicio, Proyectos informáticos no lleguen a cumplirse en el tiempo establecido. Uso inadecuado de los Equipos TI. Requerimientos mal definidos.
Gestión, Comunicación Interna y Externa	Desconfiguración del Servidor de Correos. Hardware en mal estado. Mala calidad de Servicios

AUDITORÍA INFORMÁTICA

Caso: EMPRESA DE SERVICIOS DE CONSULTORÍA EN TI

Factores de Riesgos	Consecuencia Real	Consecuencia Potencial
Servidor de Aplicaciones fuera de servicio.	No existe desarrollo alguno.	Proyectos fuera de Plazo
Proyectos informáticos no lleguen a cumplirse en el tiempo establecido.	Mala imagen de la empresa.	Multas por atrasos.
Uso inadecuado de los Equipos TI.	Pérdida, rotura, fallas, económica	Sin avance en Proyectos, Efecto negativo áreas de la empresa.
Requerimientos mal definidos.	Sistema desarrollado no cumple expectativas del cliente, económica	Tiempo perdido, Costo excesivo, Imagen Empresa, Perdida de cliente
Desconfiguración del Servidor de Correos.	Sin comunicación interna y externa	Imagen empresa, Sin información para la toma de decisiones
Hardware en mal estado.	Compra de nuevo Hardware	Perdida de información, inconsistencia de datos
Mala Calidad de Servicios.	Imagen empresa	Perdida de fidelización del cliente

AUDITORÍA INFORMÁTICA

Caso: EMPRESA DE SERVICIOS DE CONSULTORÍA EN TI

Consecuencias				Probabilidad				
			NG	A	B	C	D	E
Imagen	Económica	Clientes		No ha ocurrido en la Industria (Sector)	Ha ocurrido en la Industria (Sector)	Ha ocurrido en la Empresa	Sucede varias veces por año en la Empresa	Sucede varias veces por año en la Unidad
Impacto potencial	*Catastrófica*	*Totalmente descontento*	5	*M*	*M*	*A*	*MA*	*MA*
Impacto Grave	*Severo*	*Supervisión constante*	4	*M*	*M*	*A*	*MA*	*MA*
Impacto mediano	*Grave*	*Supervisión Mediana*	3	*M*	*M*	*A*	*A*	*A*
Impacto Leve	*Leve*	*Supervisión Leve*	2	*M*	*M*	*M*	*M*	*M*
Impacto muy leve	*Marginal*	*Sin Supervisión*	1	*B*	*B*	*B*	*B*	*B*
Sin Impacto	*Sin Efecto*	Sin Efecto	0	*N*	*N*	*N*	*N*	*N*

AUDITORÍA INFORMÁTICA

Caso: EMPRESA DE SERVICIOS DE CONSULTORÍA EN TI

Tabla Imagen

Nivel	*Descripción*
0	*Sin impacto*
1	*Impacto muy leve, deja en manifiesto descoordinación inter-empresa*
2	*Impacto leve, puede ser remediado sin afectar la relación con el cliente*
3	*Impacto mediano, multas por incumplimiento de plazos, afecta sólo a algunos clientes*
4	*Impacto Grave, multas implican más de un clientes, se comenta en el medio*
5	*Impacto potencialmente grave, peligra actuales y futuros clientes.*

AUDITORÍA INFORMÁTICA

Caso: EMPRESA DE SERVICIOS DE CONSULTORÍA EN TI

Tabla Económica

Nivel	Descripción
0	*Sin Efecto*
1	*Marginal (menos de 10 mil dólares - daños leves), Sin interrupción en las actividades de producción, mantenimiento, puesta en marcha, etc.).*
2	*Importante (de 10 mil a 100 mil dólares - daños menores), Interrupción breve de las actividades. Impacto Leve.*
3	*Grave (de 100 mil a 1 millón de dólares - daños locales), Pérdidas económicas por parada temporal, lucro cesante o responsabilidad civil.*
4	*Severo (de 1 millón a 10 millones de dólares - daños mayores), Pérdida parcial en las operaciones o de la planta desde uno hasta 10 millones de dólares*
5	*Catastrófica (más de 10 millones de dólares - daños generalizados): Pérdida total o sustancial en la producción, en la infraestructura, etc.*

AUDITORÍA INFORMÁTICA

Caso: EMPRESA DE SERVICIOS DE CONSULTORÍA EN TI

Tabla Clientes

Nivel	*Descripción*
0	*Sin Efecto*
1	*Cliente asume actividades como normales y cotidianas, Sin Supervisión.*
2	*Cliente asume situación circunstancial. Supervisión leve*
3	*Cliente esporádicamente remite observaciones, supervisión mediana*
4	*Reuniones y supervisión constante por parte del cliente, generando remediales.*
5	*Cliente totalmente descontento y puede poner fin a Contrato, desea recuperar su inversión*