Su futuro es nuestra energía

Gestión de riesgos, experiencias aplicando dos enfoques metodológicos.

Seguridad Informática
División Sistemas de Información

AÑOS

La energía que nos une

Temario

- Conceptos de Riesgo.
- Normas ISO 31000 y 27005.
- Gestión de riesgos
- Experiencias utilizando dos metodologías

Riesgo

Riesgo

Posibilidad que un evento nos afecte negativamente
(definición ISO 31000)

Lograr "cero riesgo" no es posible por lo cual se hace necesario conocerlo, tratarlo y convivir con el.

El análisis de riesgos es una **herramienta de gestión** para la toma de decisiones y un justificativo para invertir en seguridad, procedimientos y tecnología.

Normas ISO

ISO-31000

Define un marco de trabajo general para la gestión del riesgo **aplicable en cualquier ámbito**.

ISO-27005

Guía para la gestión del riesgo **enfocado en la Seguridad de la Información (TI).**

Conceptos

Activos

Elementos con valor tangible o intangible para la organización.

Amenaza

Agentes capaces de causar daños a los activos aprovechando sus vulnerabilidades.

Vulnerabilidad

Debilidad (características o defectos) asociados con un activo.

Conceptos

Probabilidad

Frecuencia con la cual un riesgo o amenaza pueda ocurrir.

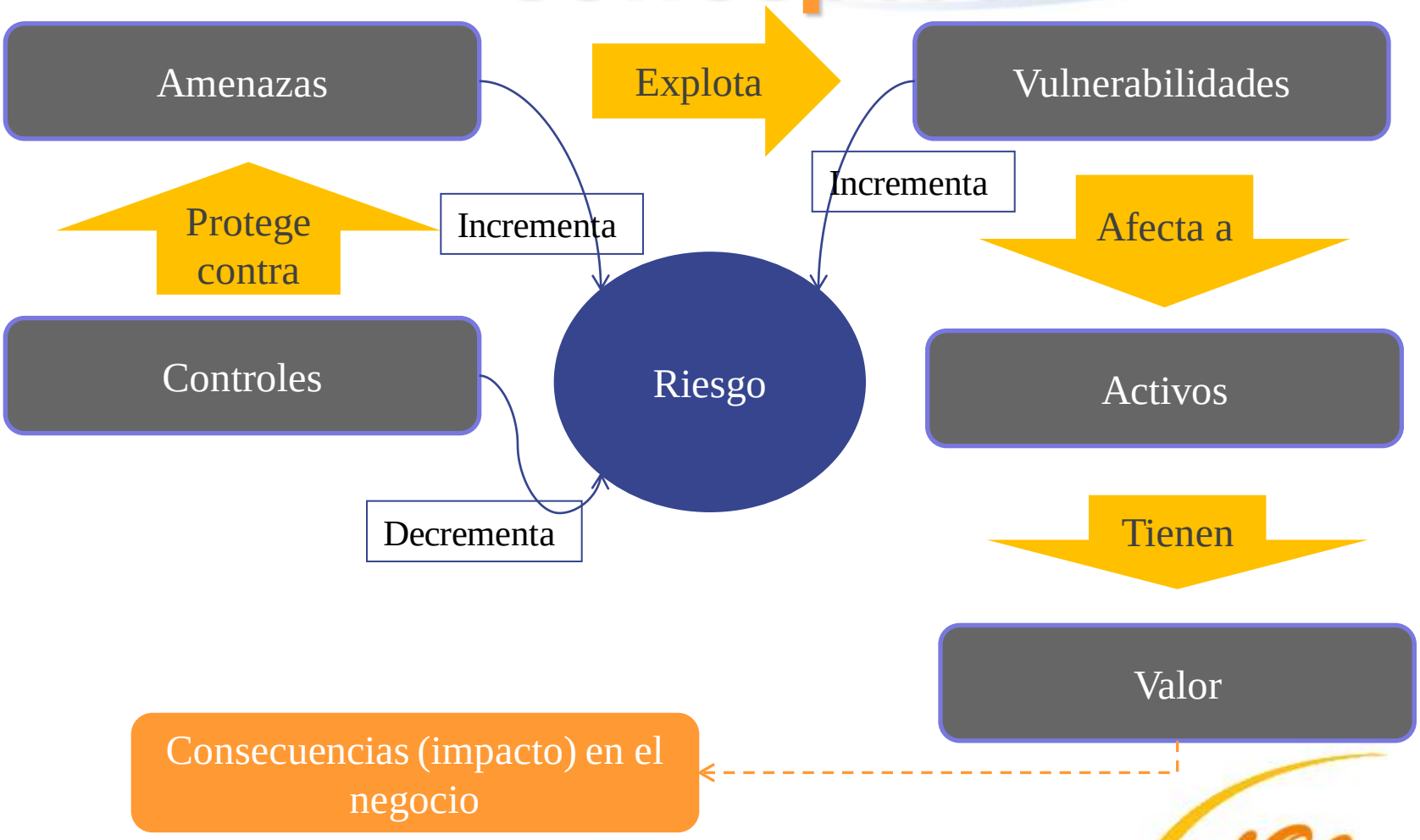
Impacto

Consecuencia del riesgo.

Control

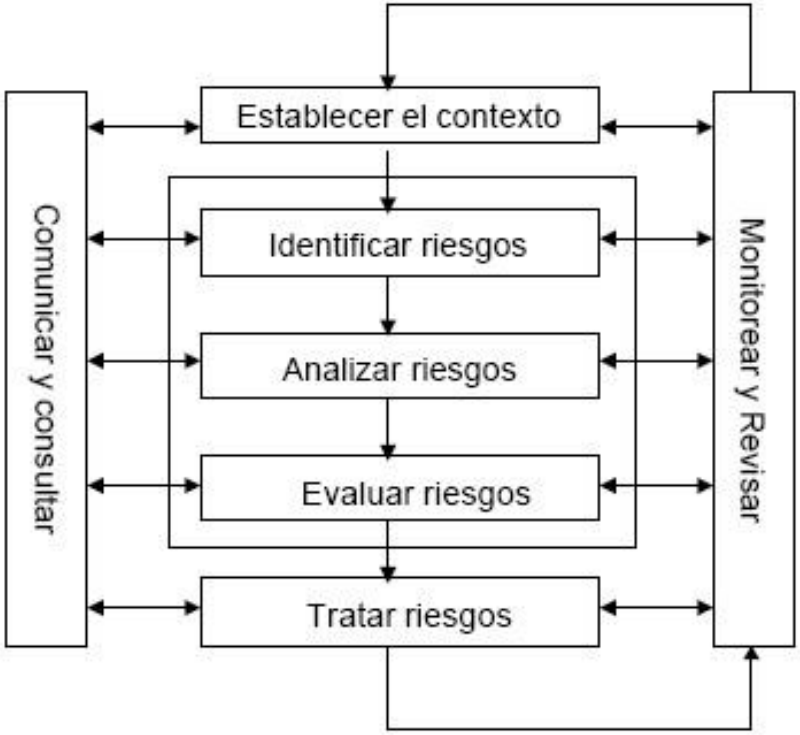
Medida que intenta disminuir el riesgo.

Conceptos


Amenazas
Explota
Vulnerabilidades
Incrementa
Protege contra
Incrementa
Afecta a
Controles
Riesgo
Activos
Decrementa
Tienen
Valor
Consecuencias (impacto) en el negocio

Gestión del Riesgo

Norma ISO 31000



Gestión del Riesgo

Apoyo de la Dirección

El análisis necesita recursos humanos.

Tratar el riesgo puede necesitar presupuesto disponible.

Establecer el contexto

Definir el alcance.

Gestión del Riesgo

Establecer el contexto

Definición de equipos de trabajo (roles y responsabilidades, conocimiento de los procesos, áreas de TI y metodología).

Visión de la situación actual.

Metodología a utilizar.

No existe un modelo único, depende de los recursos disponibles, la complejidad de la organización y cuan preciso se desea sea el resultado.

Gestión del Riesgo

Establecer el contexto

Elaboración de la Política de Riesgos (alcance, metodología, valoración de probabilidad e impacto, valor del riesgo tolerable).

Identificar los Riesgos

Elaborar la lista de objetivos, activos o procesos.
Identificar el conjunto de riesgos asociados a cada uno de ellos y los controles que estén ya implementados.

Gestión del Riesgo

Evaluar (valorar) el Riesgo

Surge de la *probabilidad* y el *impacto*.

Gestión del Riesgo

Tratamiento del Riesgo

Mitigar

Definición de nuevos controles que permitan disminuir la probabilidad y/o el impacto.

Transferir

Se transfiere el riesgo a terceros.

Gestión del Riesgo

Tratamiento del Riesgo

Asumir

Existen factores por los cuales se asume el riesgo:

No disponer de presupuesto para mitigarlo o transferirlo.

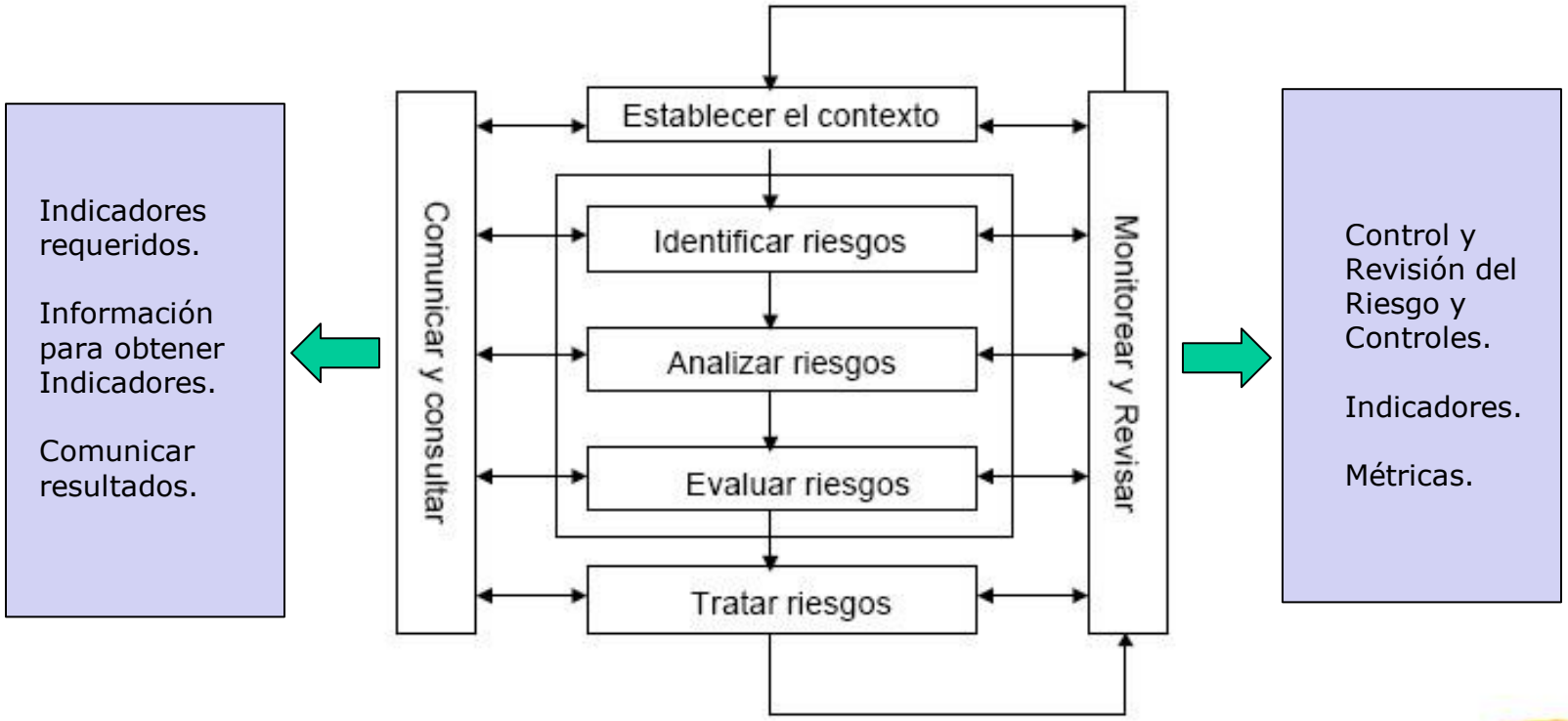
Se encuentra dentro del nivel de riesgo tolerable.

Abandonar

No continuar con la actividad que genera el riesgo.

Gestión del Riesgo

Análisis del Riesgo



Su futuro es nuestra energía

Experiencia de aplicación de dos metodologías de gestión de riesgo

Metodologías de análisis de riesgo

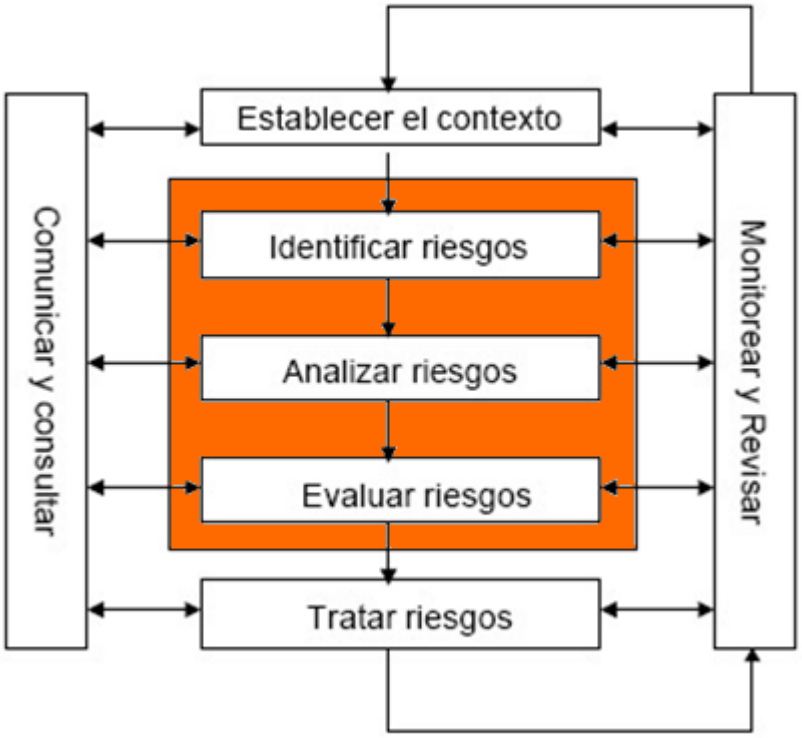
2005 al 2010 – Gestión de riesgo **basados** en la metodología GIRO

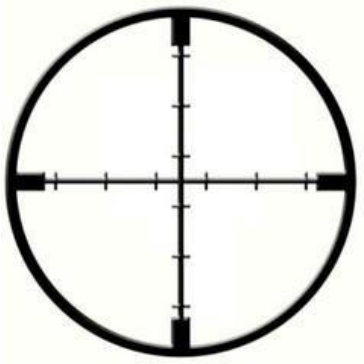
Metodología 1

2011 – Gestión de riesgo **basados** en el enfoque COSO II

Metodología 2

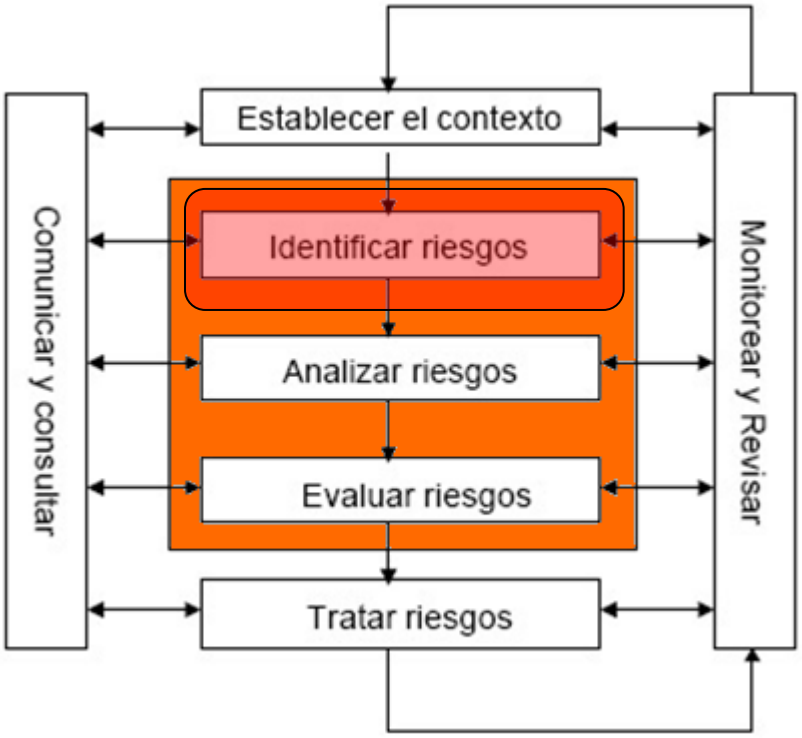
Gestión de Riesgo

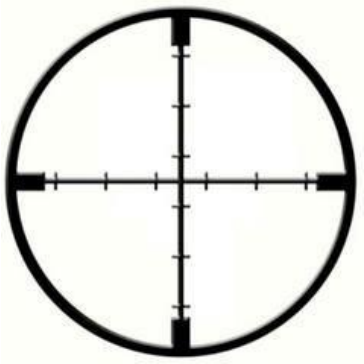




Valoración del riesgo

Gestión de Riesgo





Valoración del riesgo

Identificar el riesgo M1

Identificación de recursos que pueden ser afectactados por las amenazas (agentes de riesgo).

Identificar el riesgo M1

Identificación de las amenazas → **Identificación de recursos que pueden ser afectados por las amenazas** → **Identificación de controles existentes**

- Tablas de amenazas incluidas en la metodología
- Tablas de amenazas de Magerit
- **Talleres de trabajo**

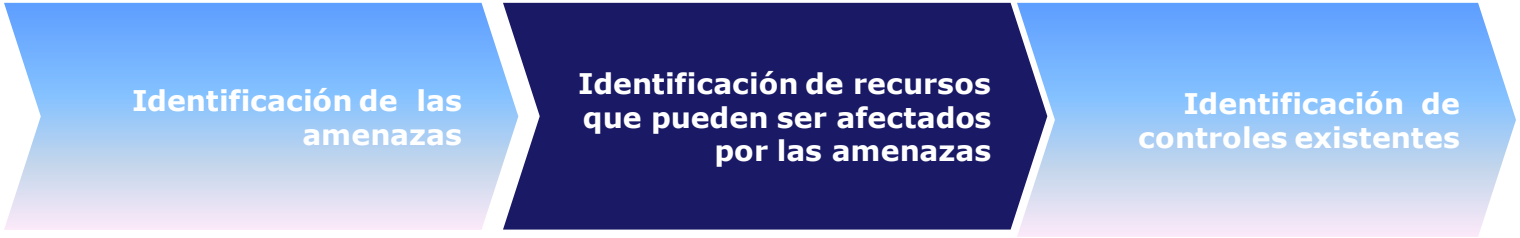
Ej. Lista de amenazas

- Fuego
- Explosión
- Desastres industriales
- Avería de origen físico o lógico
- Corte del suministro eléctrico
- Errores de los usuarios
- Errores de monitorización
- Difusión de software dañino

.....

.....

Identificar el riesgo M1



- Inventarios de activos
- **Talleres de trabajo**

Ej. Lista de recursos

- LOCALES
  - Edificio CPD 1
  - Local Cuareim
  - Palacio de la LUZ
- HARDWARE
  - Servidores Mainframe OS 390
  - Servidores Windows críticos
- COMUNICACIONES
  - Equip. de comunicaciones CPD
- PERSONAL
  - Personal SIS
  - Personal SIS Contratado
  - .....

Identificar el riesgo M1

Escenario de riesgo

• Unidad de análisis básica de la metodología
•Representa una situación en la cual **un recurso** determinado está **expuesto a una amenaza** específica de posible ocurrencia.

Escenario de riesgo = (recurso, amenaza)

Listado de escenarios de riesgos.

Identificar el riesgo M2

Identificación de riesgos que pueden afectar a la capacidad de alcanzar los objetivos definidos.

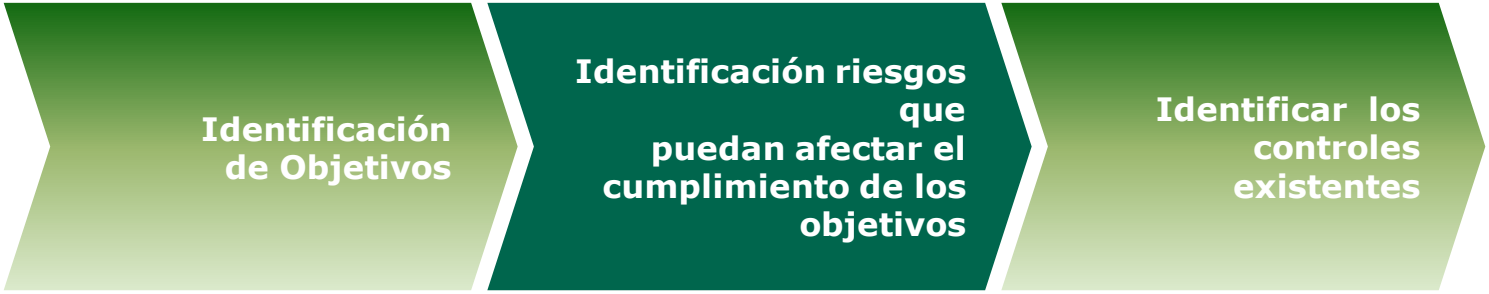
Identificar el riesgo M2

- Objetivos de la organización (Alineación de TI con el Negocio)
- **Entrevistas con expertos, talleres**

Ej. Lista de objetivos

- Garantizar el conocimiento adecuado de la metodología de gestión de proyectos
- Planificar adecuadamente la carga actual y futura.
- Monitorear el cumplimiento de las políticas de seguridad
- Garantizar un adecuado nivel de motivación del personal

Identificar el riesgo M2



- **Entrevistas con expertos, talleres**

Objetivo: Garantizar el conocimiento adecuado de la metodología de gestión de proyectos

Ej. Riesgos que afectan al objetivo

•No contar con instancias de capacitación en las disciplinas de gestión de proyectos

•No lograr identificar las debilidades del personal en las áreas conocimiento de Gestión de Proyectos

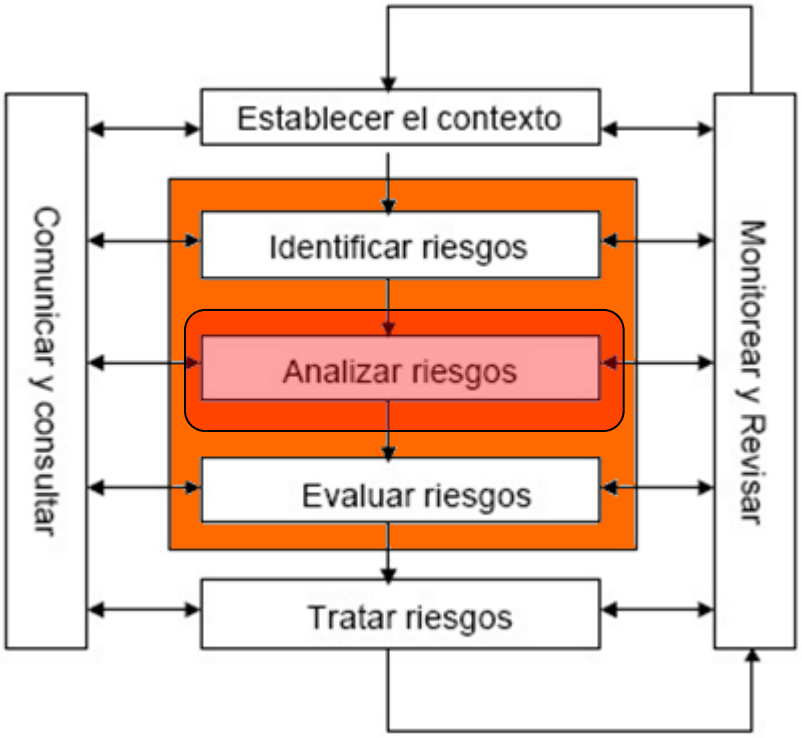
Identificar el riesgo M2

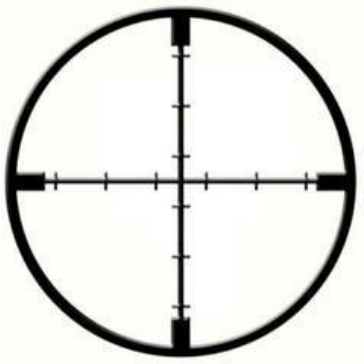
Unidad de estimación de riesgo

- Unidad de análisis
- Representa una situación en la cual el **cumplimiento de un objetivo** determinado se **puede ver afectado por un evento**.

Escenario de riesgo= (objetivo, riesgo)

Gestión de Riesgo





Valoración del riesgo

Analizar el riesgo

Valor del Riesgo = Combinación del valor de Probabilidad de ocurrencia y del impacto

Se listan escenarios de riesgo y se asignan valores a la probabilidad y al impacto.

Analizar el riesgo el riesgo: M1

- **Probabilidad de ocurrencia de la amenaza.**

- **Determinación del Impacto en términos de:**

  - Víctimas
  - Pérdidas Económicas
  - Afectación a la Operación
  - Pérdida de Información

Factores de medición de impacto

Analizar el riesgo:M1

		Evaluación de Escenarios 2009 (PERSONAS)						
		Escenario						
	C	Amenaza	Recurso	Explicación	Frecuenc	Consecuencia	Riesgo	V
4	1	Desastres biológicos	Personal SIS	Pandemia	3	2	6	
5	2	Desastres biológicos	Personal Contratado	Pandemia	3	2	6	
6	3	Desastres biológicos	Personal CPD	Pandemia	3			

Ej. De estimación en Factor personas

- Escala para frecuencia de la amenaza (probabilidad de ocurrencia)
- Para cada factor de riesgo existe una tabla de valoración
- Formula de para calculo de riesgo

Analizar el riesgo: M2

- **Probabilidad de ocurrencia del riesgo.**
- **Determinación del Impacto evaluando sin controles y con controles (riesgo inherente y riesgo residual)**

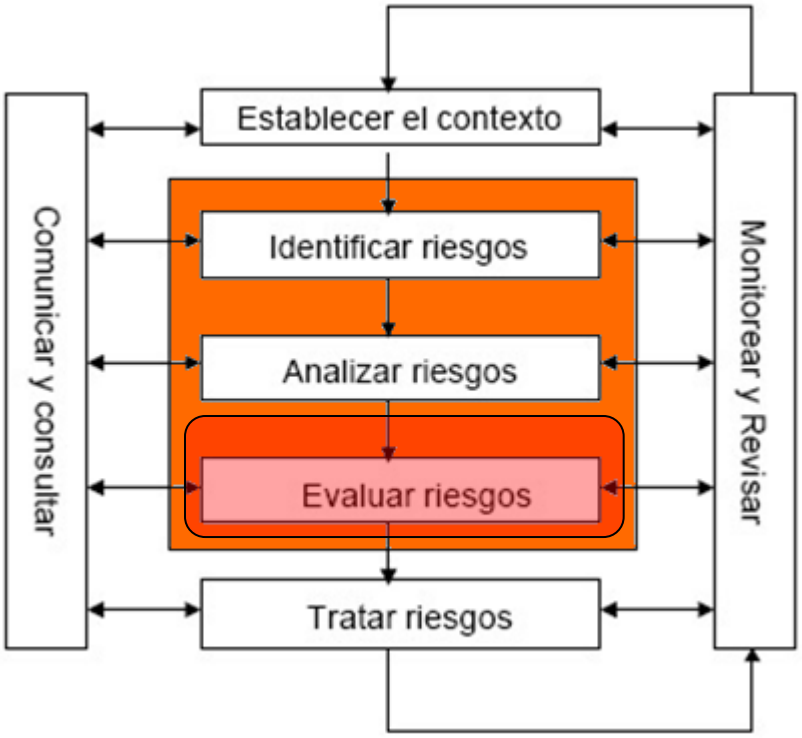
Analizar el riesgo: M2

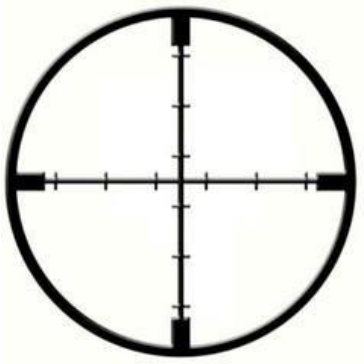
Objetivo
Garantizar el conocimiento adecuado de la metodología de gestión de proyectos

	Inherente			Residual		
	Impacto	Probabilidad	Exposición	Impacto	Probabilidad	Exposición
Riesgo						
No contar con instancias de capacitación en las disciplinas de gestión de proyectos	Bajo	Baja	2	Bajo	Muy baja	1,6
Controles				**Area**		
Se han realizado cursos de capacitación para todo el personal como mínimo hasta nivel de jefaturas				Planificación		
Riesgo						
No lograr identificar las debilidades del personal en las áreas de conocimiento de Gestión de Proyectos	Bajo	Alta	2,8	Bajo	Muy baja	1,6
Controles				**Area**		
El área de Planificación se reúne con todos los sectores de la División para determinar las necesidades de capacitación				Planificación		

- **Escala para probabilidad de riesgo**
- **Tabla de valoración del Impacto**
- **Formula de para calculo de riesgo**

Gestión de Riesgo





Valoración del riesgo

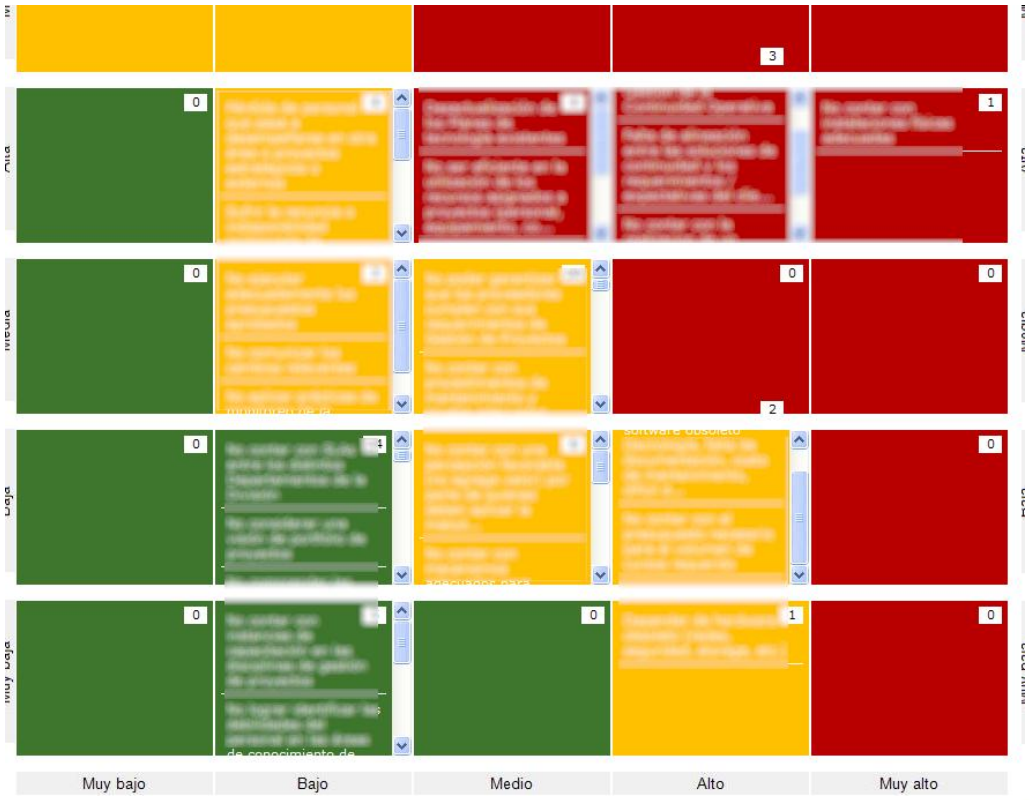
Evaluar el riesgo

- Consiste en listar los **riesgos priorizados** de acuerdo a los criterios de valoración de riesgo.

- Matriz de priorización: permite visualizar cuales riesgos requieren de un tratamiento inmediato.

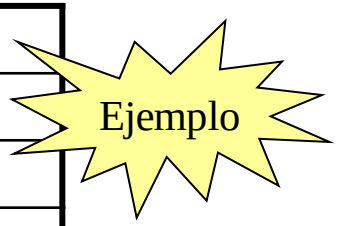
- Las decisiones tomadas en la actividad de valoración de riesgo están basadas principalmente en el nivel de **riesgo aceptable.**

Evaluar del riesgo



Escala de determinación de Probabilidad de ocurrencia

1	Muy baja	Menos de 1 vez cada 20 años
2	Baja	1 vez entre 5 y 20 años
3	Media	1 vez entre 1 y 5 años
4	Alta	Entre 1 y 12 veces al año
5	Muy alta	Más de 12 veces al año



Escala de valoración consecuencias operacionales

Valor	Nivel	Afectación / Suspensión
1	Insignificante	Menos de 3 horas
2	Marginal	Entre 3 horas y 1 día
5	Grave	Entre 2 días y 5 días
10	Crítico	Entre 6 días y 15 días
20	Desastroso	Entre 16 días y 30 días
50	Catastrófico	Más de 30 días

Ejemplo

Escala de valoración perdida de información

Valor	Nivel	Afectación / Pérdida de Información
1	Insignificante	Hasta 10% de inf. no crítica
2	Marginal	Entre 10 y 30% de inf. no crítica
5	Grave	Más del 30% de inf. no crítica
10	Crítico	Hasta 10% de inf. crítica
20	Desastroso	Entre 10 y 30% de inf. crítica
50	Catastrófico	Más del 30% de inf. crítica

Ejemplo

Preguntas...

Muchas gracias...