Ingeniería de Sistemas

# Fundamentos de estimación del riesgo

Seguridad de Sistemas de TI

2022-1

UNIVERSIDAD DE LIMA

# Agenda

I. Valor, Amenazas y Riesgo

II. Consideraciones sobre el Riesgo

III. Riesgo Cualitativo

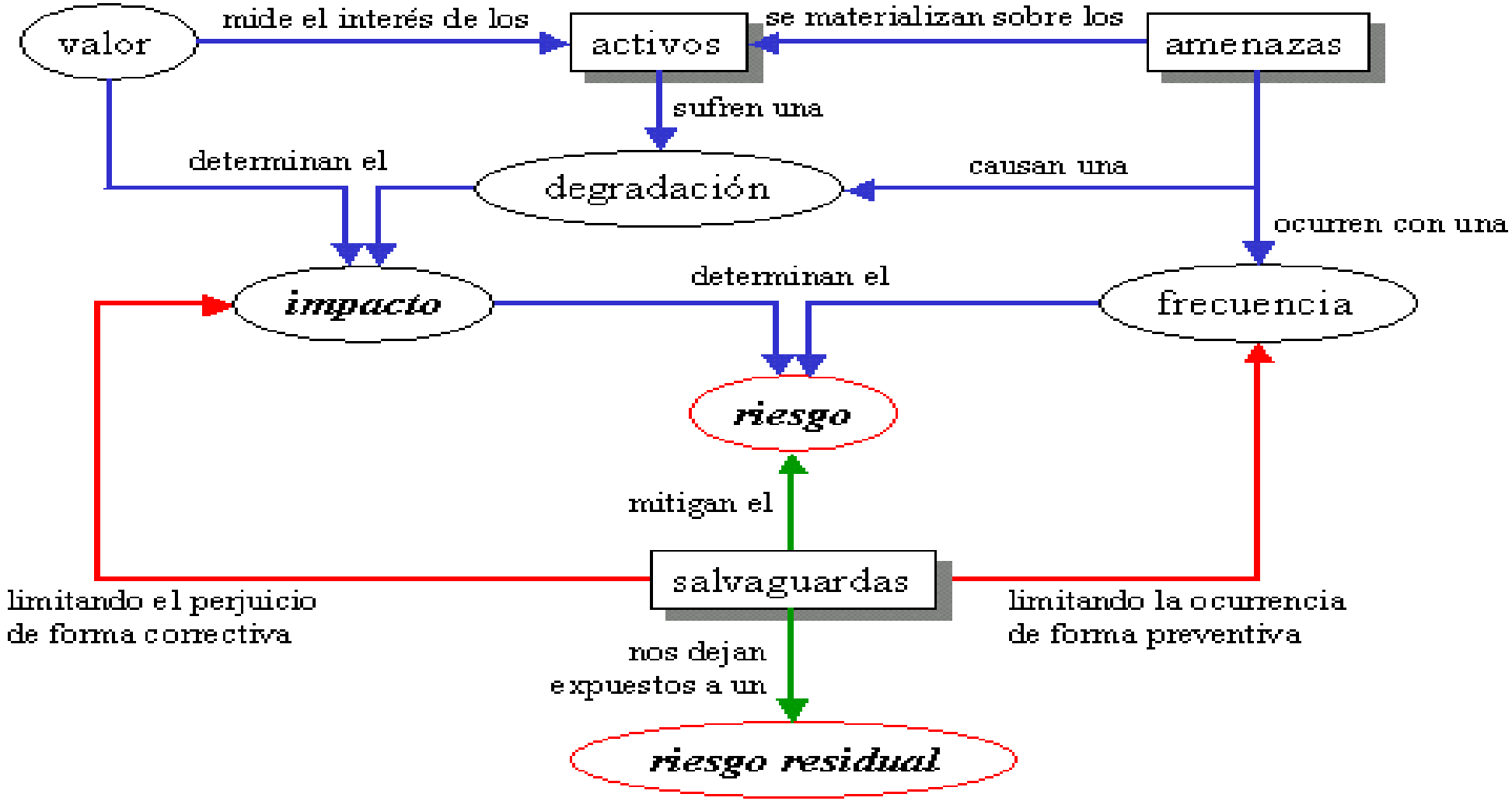
IV. Riesgo Cuantitativo

V. Conclusiones

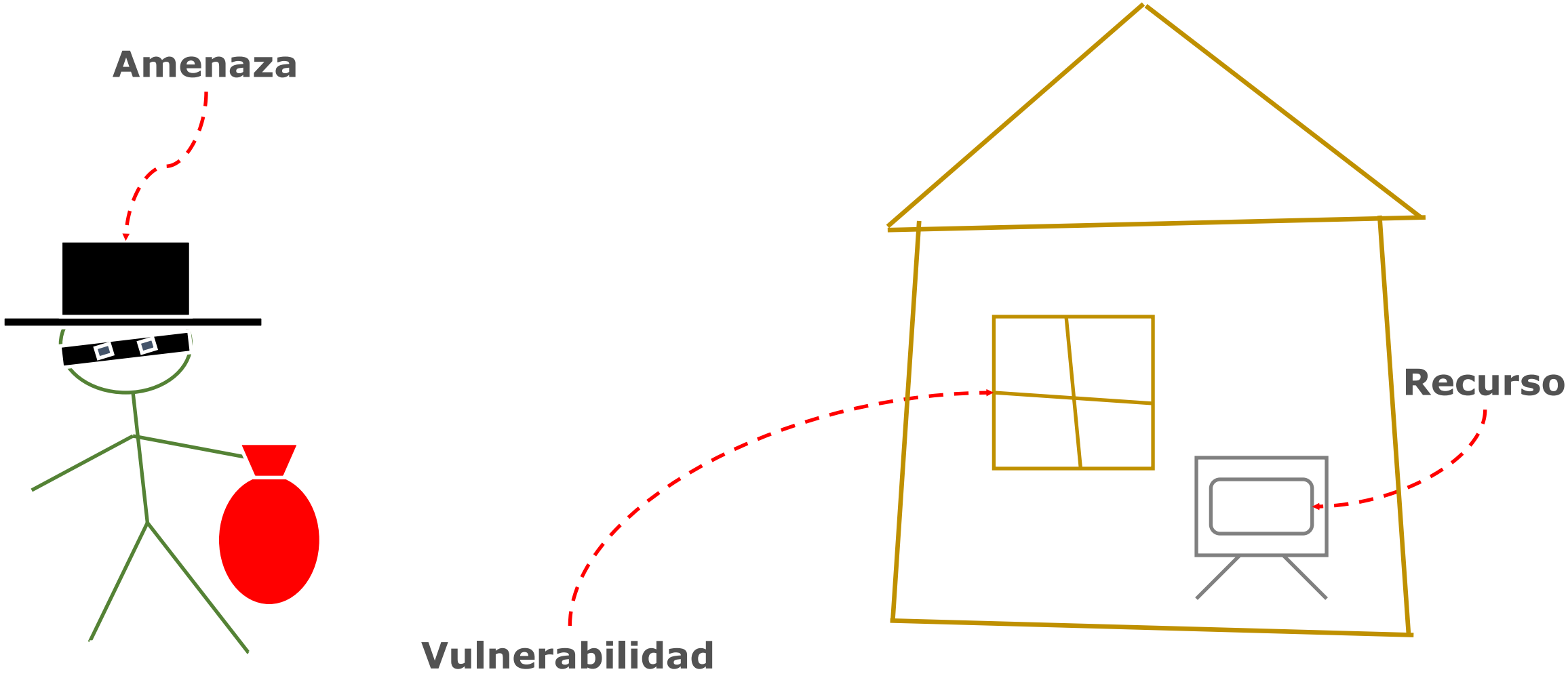
UNIVERSIDAD DE LIMA

# I. valor, amenazas y riesgo

# ¿Cómo se relacionan el Valor, las Amenazas y el Riesgo?

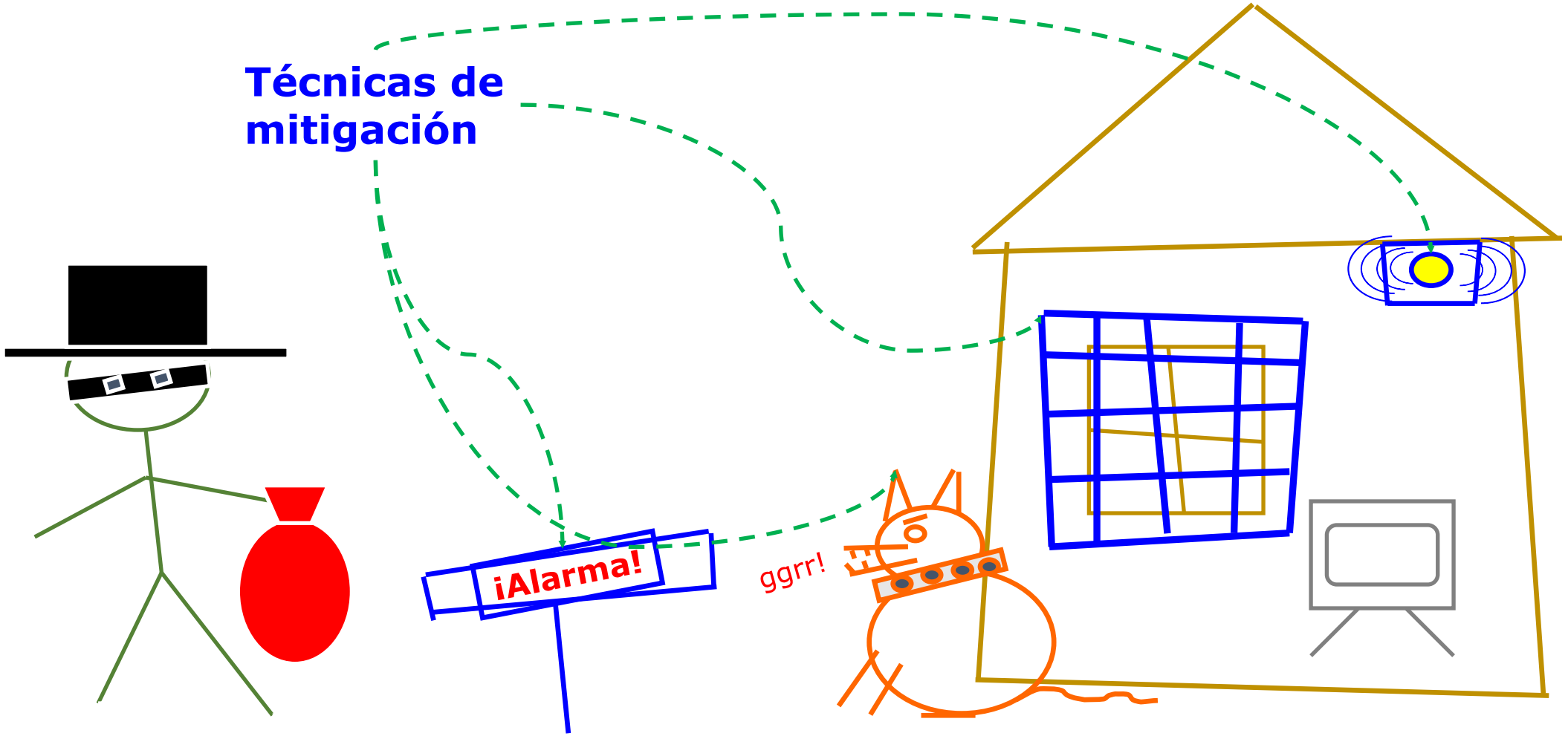


# Análisis de riesgos



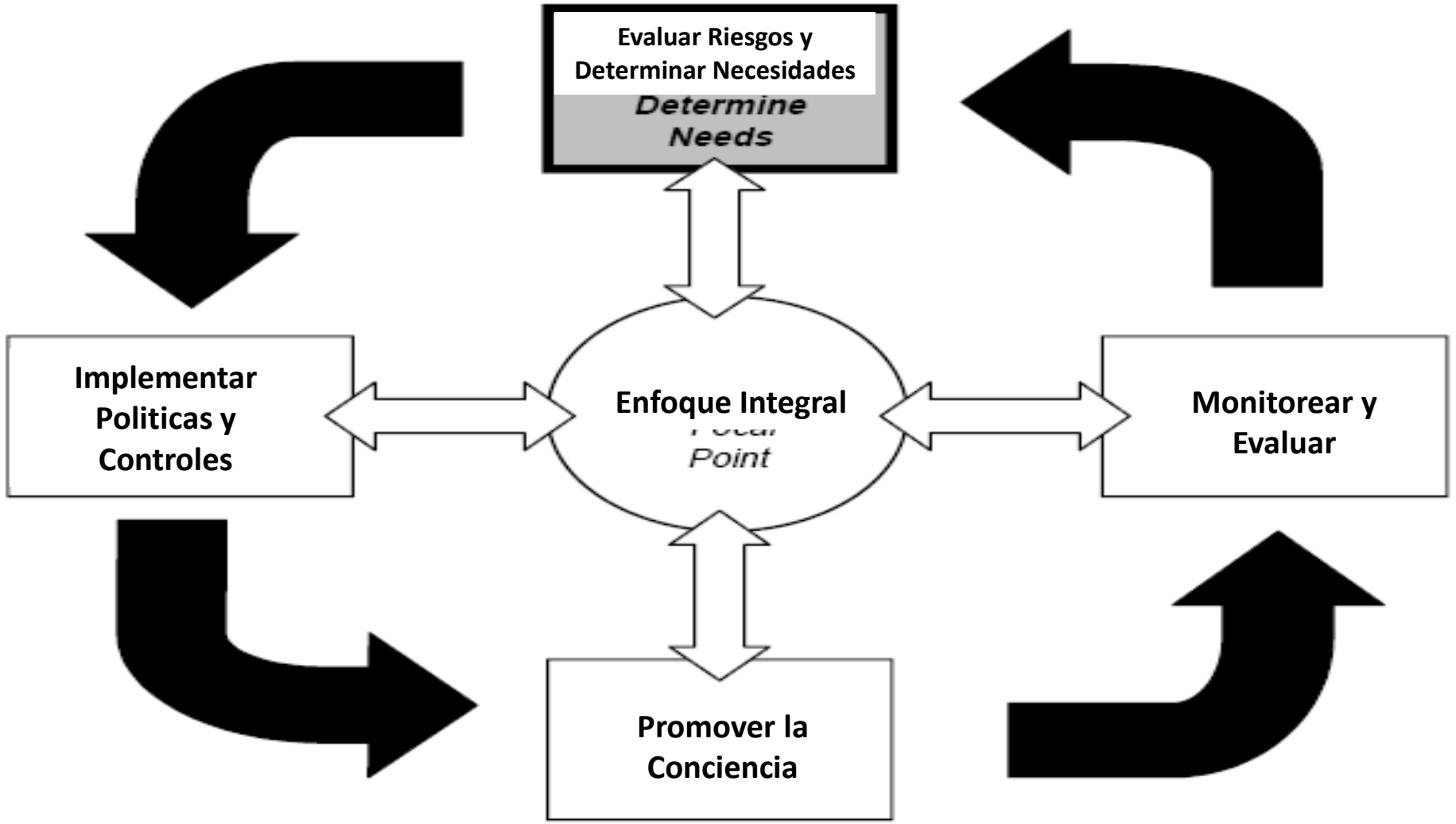

UNIVERSIDAD DE LIMA

# Despliegue de contramedidas




UNIVERSIDAD DE LIMA

# Ciclo de Gestión del riesgo




UNIVERSIDAD DE LIMA

# II. Consideraciones sobre el riesgo

# Consideraciones sobre el riesgo (I)

- Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos de ella.
- El gasto en los controles es necesario compararlo con el probable perjuicio que resulte de fallas en la seguridad
- Las técnicas de evaluación de riesgos se pueden aplicar a toda la organización, o solamente a partes de ella, como también a los sistemas de información individuales, componentes específicos de un sistema o servicios, cuando sea práctico, realista y útil

# Consideraciones sobre el riesgo (II)

➢La evaluación del riesgo es la consideración sistemática de:

- El probable perjuicio al negocio que resulte de una falla en la seguridad, tomando en cuenta las consecuencias potenciales de una pérdida de confidencialidad, integridad o disponibilidad

- La probabilidad realista de que tal falla ocurra, en vista de las amenazas y vulnerabilidades efectivas, y los controles actualmente implementados

# Consideraciones sobre el riesgo (III)

- Los resultados de esta evaluación serán una guía y determinarán la acción de una gestión apropiada, así como las prioridades de la gestión de los riesgos de seguridad de la información, y la selección de la implementación de controles para protegerla de estos riesgos
- Puede ser necesario realizar varias veces el proceso de evaluación de los riesgos y seleccionar los controles para cubrir diferentes partes de la organización o sistemas de información individuales

UNIVERSIDAD DE LIMA

# Consideraciones sobre el riesgo (IV)

- Es importante realizar revisiones periódicas de los riesgos de seguridad e implementar controles para:
  - **Tomar en cuenta los cambios en las prioridades y requisitos del negocio**
  - **Considerar nuevas amenazas y vulnerabilidades**
  - **Confirmar que los controles permanecen efectivos y apropiados**

# Consideraciones sobre el riesgo (V)

- Las revisiones se deberían realizar en diferentes niveles de profundidad, dependiendo de los resultados de las evaluaciones previas y de los cambios de niveles de riesgo que la dirección está preparada para aceptar

- Las evaluaciones de riesgo, a menudo se realizan primero a alto nivel, como una forma de priorizar los recursos en áreas de alto riesgo, y luego en un nivel más detallado, para abordar riesgos específicos

# Factores críticos para el éxito (I)

- Política, objetivos y actividades de Seguridad *que reflejen los objetivos del negocio*
- Una aproximación para la implementación de la seguridad que sea *consistente con la cultura organizacional*
- Apoyo visible y *compromiso de la alta dirección*
- Buen *entendimiento de los requisitos de seguridad*, evaluación y gestión del riesgo
- *Difusión efectiva de la seguridad* por todos los directivos y empleados

# Factores críticos para el éxito (II)

- *Distribución de las normas* y de la guía de la política de seguridad de la información a todos los empleados y personal externo
- Provisión de *entrenamiento* y educación adecuada
- Utilización de un *sistema de medición* equilibrado y completo para evaluar el comportamiento de la gestión de seguridad de la información y la realimentación de sugerencias para su mejoramiento

UNIVERSIDAD DE LIMA

# Tipos de estimación de riesgo

## ➢Cualitativo

- La técnica incluye la intuición, el juicio y la experiencia de quienes lo aplican. Permite estimar las pérdidas potenciales relacionando 4 elementos principales: las **amenazas**, las **vulnerabilidades** (que potencian el efecto de las amenazas), el **impacto** asociado a una amenaza (que indica los daños sobre un activo) y **los controles** o salvaguardas (para minimizar las vulnerabilidades o el impacto).

## ➢Cuantitativo

- Basado en dos parámetros fundamentales: la probabilidad de que un suceso ocurra y una estimación del costo o pérdidas en caso de que así sea. Este método es el menos usado ya que en muchos casos implica cálculos complejos o datos difíciles de estimar.

# III. Riesgo cualitativo

# Matriz de estimación de riesgo cualitativo (I)

| Areas of vulnerability and possible effects of damage | Risk of monetary loss | | | Risk of productivity loss | | | Risk of loss of customer confidence | | |
|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L |
| **Personnel** | | | | | | | | | |
| Unauthorized disclosure, modification, or destruction of information | | | | | | | | | |
| Inadvertent modification or destruction of information | | | | | | | | | |
| Nondelivery or misdelivery of service | | | | | | | | | |
| Denial or degradation of service | | | | | | | | | |

UNIVERSIDAD DE LIMA

# Matriz de estimación de riesgo cualitativo (II)

| Areas of vulnerability and possible effects of damage | Risk of monetary loss | | | Risk of productivity loss | | | Risk of loss of customer confidence | | |
|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L |
| **Facilities and equipment** | | | | | | | | | |
| Unauthorized disclosure, modification, or destruction of information | | | | | | | | | |
| Inadvertent modification or destruction of information | | | | | | | | | |
| Nondelivery or misdelivery of service | | | | | | | | | |
| Denial or degradation of service | | | | | | | | | |

UNIVERSIDAD DE LIMA

# Matriz de estimación de riesgo cualitativo (III)

| Areas of vulnerability and possible effects of damage | Risk of monetary loss | | | Risk of productivity loss | | | Risk of loss of customer confidence | | |
|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L |
| **Applications** | | | | | | | | | |
| Unauthorized disclosure, modification, or destruction of information | | | | | | | | | |
| Inadvertent modification or destruction of information | | | | | | | | | |
| Nondelivery or misdelivery of service | | | | | | | | | |
| Denial or degradation of service | | | | | | | | | |

UNIVERSIDAD DE LIMA

# Matriz de estimación de riesgo cualitativo (IV)

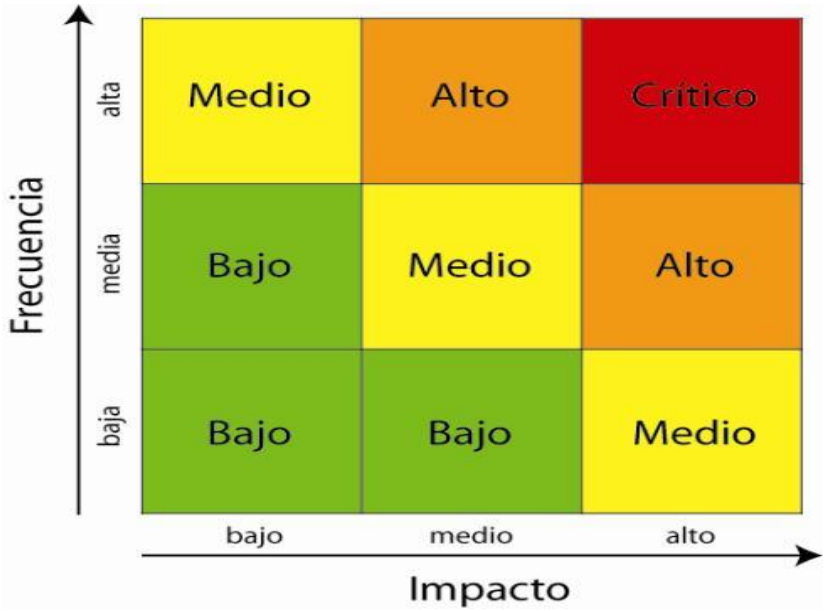
| Areas of vulnerability and possible effects of damage | Risk of monetary loss | | | Risk of productivity loss | | | Risk of loss of customer confidence | | |
|---|---|---|---|---|---|---|---|---|---|
| | H | M | L | H | M | L | H | M | L |
| **Communications** | | | | | | | | | |
| Unauthorized disclosure, modification, or destruction of information | | | | | | | | | |
| Inadvertent modification or destruction of information | | | | | | | | | |
| Nondelivery or misdelivery of service | | | | | | | | | |
| Denial or degradation of service | | | | | | | | | |
| **Software and operating systems** | | | | | | | | | |
| Unauthorized disclosure, modification, or destruction of information | | | | | | | | | |
| Inadvertent modification or destruction of information | | | | | | | | | |
| Nondelivery or misdelivery of service | | | | | | | | | |
| Denial or degradation of service | | | | | | | | | |

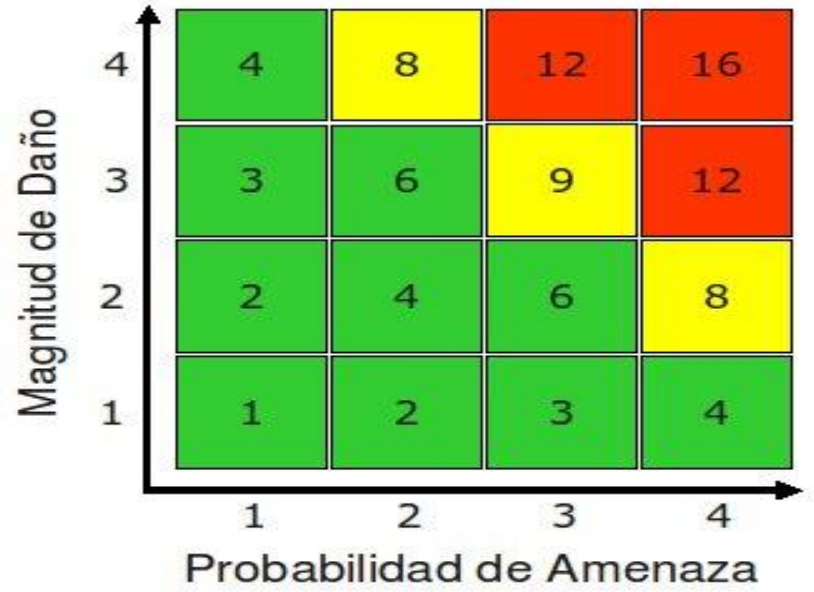
UNIVERSIDAD DE LIMA

# Matriz de estimación de riesgo cualitativo (V)

| | Risk category | | | |
|---|---|---|---|---|
| Areas of vulnerability | Monetary loss | Productivity loss | Loss of customer confidence | Overall risk |
| Personnel | | | | |
| Facilities and equipment | | | | |
| Applications | | | | |
| Communications | | | | |
| Software and operating systems | | | | |

# Matriz de estimación de riesgo cualitativo (VI)

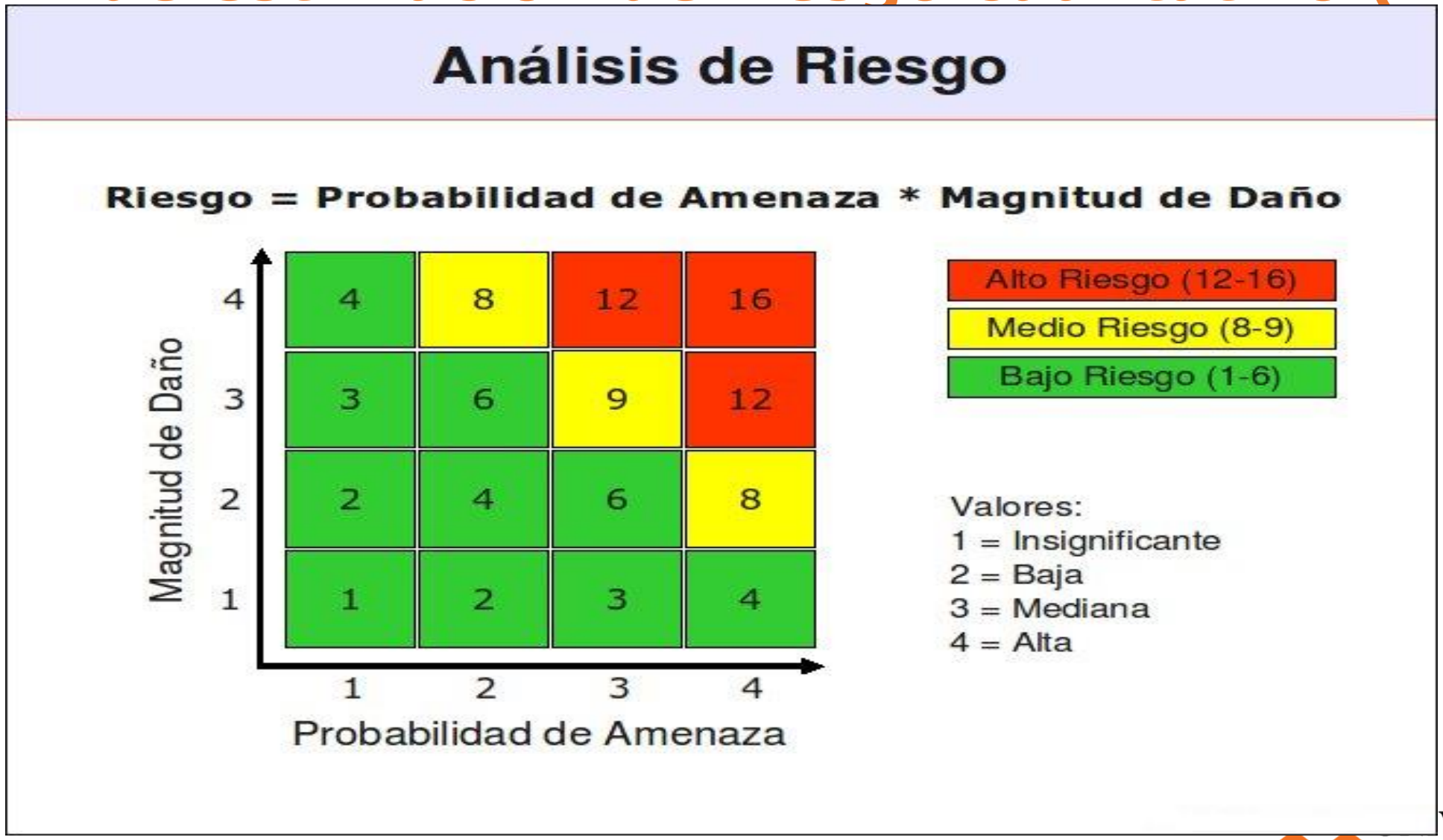



- Una matriz de riesgo constituye una herramienta de control y de gestión utilizada para identificar el tipo y nivel de riesgos inherente a las actividades (procesos y productos) más importantes de una empresa en base a factores exógenos y endógenos.

UNIVERSIDAD DE LIMA

# Matriz de estimación de riesgo cualitativo (VII)



# IV. Riesgo cuantitativo

# Análisis Costo-Beneficio y ROSI

- Evaluación del grado de reducción de riesgo que se espera alcanzar implementando políticas.

- **Beneficio neto = Beneficio – Costo**
- **ROI = (Beneficio – Costo)/Costo**

- **Beneficio neto =Riesgo reducido – Costo (inversión de control)**
- **ROSI = (Riesgo reducido – Costo)/Costo**

**Riesgo Reducido = ALE*Eficacia de control**

UNIVERSIDAD DE LIMA

# Algunas definiciones usadas para cuantificar el riesgo

- Valor de los Activos (**VA**)
  - Valor de los activos de una organización
- Frecuencia  de la Amenaza (**FA**)
  - Número de incidencias por año
- Factor de Exposición a la Amenaza (**FEA**)
  - Grado de daño que experimenta un Activo
- Eficacia de la Seguridad (**ES**)
  - Porcentaje de mitigación que tiene un Control dado sobre una Amenaza
- Costo de la Seguridad
  - Costo anual de la implementación del Control

# Algunas relaciones

- Expectativa de Pérdida Simple (EPS o SLE)
  - **Valor del Activo x Factor de Exposición**

- Expectativa Anualizada de Pérdida (EAP o ALE)
  - **Expectativa de Pérdida Simple x Frecuencia de la Amenaza**

UNIVERSIDAD DE LIMA

# Ejemplo de estimación de riesgo cuantitativo (I)

- Caso de siniestro en la organización: Se produce un incendio parcial (focalizado en un área)
  - Valor de Activos en el área: U.S. $ 200,000
  - FEA = 33%
  - FA = 0.1
  - SLE = VA **x** FEA = 200,000 x 0.33 = 66,000
  - ALE = SLE **x** FA = 66,000 * 0.1 = 6,600
  - Monto anual sustentable para aplicar controles.
  - ¿Será factible solicitar Montos superiores?

UNIVERSIDAD DE LIMA

# Ejemplo de estimación de riesgo cuantitativo (II)

Tenemos un site de e-commerce alojado en un servidor Web. La probabilidad de que este servidor falle es 20%. Este valor representaría el ARO del riesgo.

Si el site contenido en este servidor genera $100 en una hora y se estima que puede estar fuera de servicio por 2 horas mientras el sistema es reparado cuando falle, por lo tanto el costo del riesgo es $200. En adición, hay que considerar el reemplazo del servidor en si. Si el servidor cuesta $4,000 , esto incrementa el costo en $4,200.

**ALE = VI x EF x ARO**

**Leyenda:**

- ALE = Pérdida Anual Esperada
- VI = Valor de la información
- EF = Factor de Exposición
- ARO = Razón de ocurrencia Anual

**ARO =** 0,2

**SLE =** $4,200

**SLE =VI x EF**

Resultado :

ALE = 0,2 * $4200 = $840

UNIVERSIDAD DE LIMA

# Comparando enfoques de estimación de riesgo

| Propiedad | Cuantitativo | Cualitativo |
|---|---|---|
| Análisis costo/beneficio | Si | No |
| Costo ($) | Si | No |
| Puede ser automatizado | Si | No |
| Cálculos complejos | SI | No |
| Suposiciones u opiniones | Pocas | Muchas |
| Información requerida | Mucha | Poca |
| Tiempo / trabajo involucrado | Mucho | Poco |
| Facilidad de comunicación | Fácil | Difícil |

# Caso ROSI

# Cálculo del ROSI

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution}$$

UNIVERSIDAD DE LIMA

# Ejemplo: Riesgo Cuantitativo

- Acme Corp. esta considerando invertir en una solución antivirus. Cada año, Acme sufre 5 ataques de virus (ARO=5). El CISO estima que cada ataque costara aproximadamente 15.000 USD en perdida de datos y productividad (SLE=15.000). La solución de antivirus debería bloquear 80% de los ataques (ratio de mitigación=80%) y cuesta 25.000USD por año (precio de licencias 15.000USD + 10.000USD por entrenamientos, instalación y mantenimiento etc.).
- El retorno de inversión de seguridad (ROSI) para la solución se calcula de la siguiente manera:

$$ROSI = \frac{(5 * 15000) * 0.8 - 25000}{25000} = 140\%$$

- Según el calculo del ROSI, esta solución antivirus es una solución que genera beneficios.

UNIVERSIDAD DE LIMA