SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

1.3.0. Capítulo 3
Parte 1 de 2
Gestión de riesgos

JOSÉ PABLO HERNÁNDEZ

1. INTRODUCCIÓN

Hay que medir los riesgos (análisis) para decidir cómo afrontarlos (gestión).

El análisis de riesgos (AR), según se define en el método MAGERIT, es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización.

La gestión de riesgos (GR), según se define en el método MAGERIT, es la selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir, o controlar los riesgos identificados.

AGR: Análisis y gestión de riesgos.

1. INTRODUCCIÓN

El AGR es una tarea principal para la gestión de la SI, que no debe supeditarse a otras, más bien al contrario, ordena el resto de tareas que se realicen.

El AGR es la herramienta que permite ejercitar una protección responsable de los activos de información de la empresa.

Por simplicidad el AGR se suele acortar a Gestión de riesgos, pero en ningún caso este nombre corto supone eliminar la etapa inicial de análisis de riesgos.

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

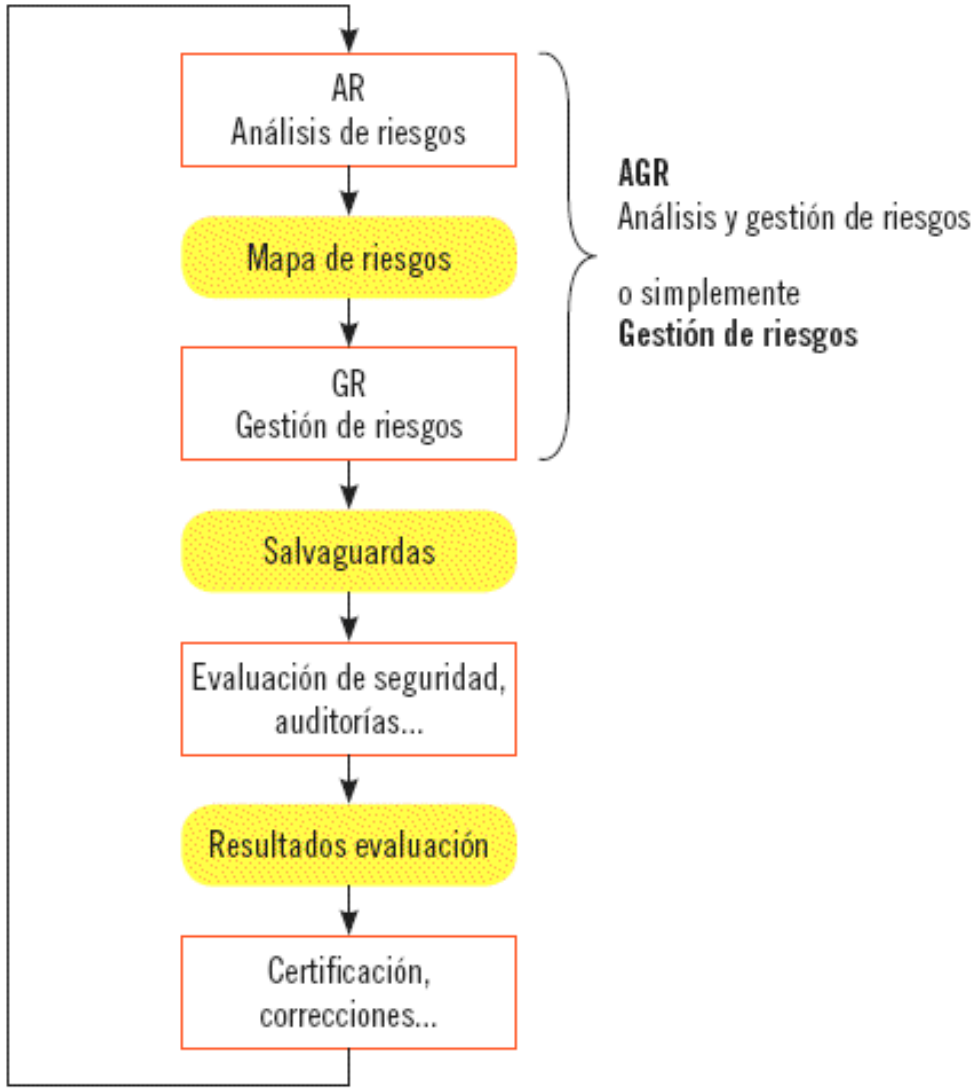
Será recomendable realizar un AGR en todas las empresas que dependan de los sistemas de información y comunicaciones para el cumplimiento de su misión.

Será necesario realizar un AGR cuando la empresa quiera obtener determinadas certificaciones de cumplimiento de normas (v.g. ISO 27001).

Será necesario realizar un AGR por precepto legal, por ejemplo, para conducir una auditoría de seguridad, o para definir el marco de cumplimiento de una ley.

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

Proceso de Gestión del riesgo, y su relación con una auditoría, orientada a obtener una certificación de cumplimiento de una norma



2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

Realizar un AGR puede ser muy costoso.

La homogeneidad es fundamental, porque resulta difícil decidir por dónde empezar (un BIA puede responder esta pregunta).

Los criterios para decidirlo deben mantenerse posteriormente.

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

La solución es sencilla:

Primero, lo más importante:

- **Máximo impacto**
- **Máximo riesgo**

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

Alternativas para tratar el riesgo:

- **Mitigar el riesgo:** la empresa puede optar por aplicar contramedidas que reduzcan el impacto de un incidente, o aplicar contramedidas para reducir la probabilidad de la amenaza.
- **Evitar el riesgo:** la empresa puede decidir eliminar los activos o servicios bajo riesgo. Puede interpretarse como una forma de mitigación extrema.
- **Transferir el riesgo:** la empresa puede mitigar el riesgo propio, trasladándoselo a otros. Por ejemplo, puede compartir el activo o función bajo riesgo con otra empresa, o subcontratar la función completamente a terceros, o contratar pólizas de seguros con empresas aseguradoras.
- **Aceptar el riesgo:** la empresa decide no hacer nada. Esta medida siempre debe autorizarla la Dirección de la empresa.

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

La decisión de una u otra acción dependerá de:

- **Requisitos legales o regulatorios,** tanto de ámbito nacional como internacional. Estos requisitos siempre deben cumplirse.
- **Requisitos operacionales,** como normas que deba cumplir la empresa.
- **Objetivos de la empresa,** como los derivados de su estrategia.
- **Rentabilidad de la acción,** comparando el coste de la acción frente al beneficio o daño probable que evita.

La seguridad total no existe

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

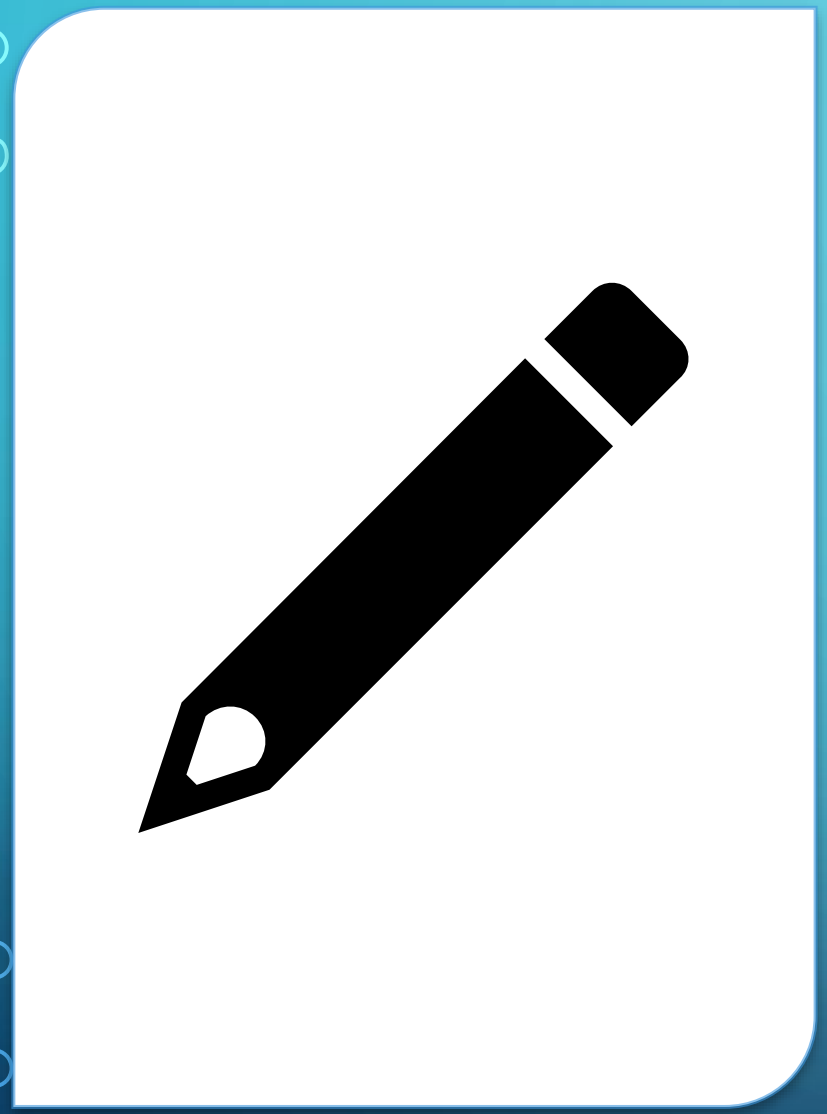
Fases de un análisis de riesgos (AR):

- **Identificar los activos y sus relaciones de dependencia.**
- **Identificar las amenazas y sus vulnerabilidades.**
- **Estimar el impacto (daño posible), y la probabilidad del mismo.**
- **Estimar el nivel de riesgo de la ocurrencia de la amenaza.**
- **Estimar el coste de mitigar el riesgo (incluyendo evitarlo o transferirlo).**

2. APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

Fases de un gestión de riesgos (GR):

- **Identificar los criterios de aceptación de riesgo (regulatorios, normativos, objetivos de la empresa, y rentabilidad).**
- **Determinar, según esos criterios, si el riesgo calculado en AR es aceptable, o si debe mitigarse.**
- **Identificar las medidas de seguridad necesarias, y evaluar la reducción de riesgo que aportan (plan de acción).**
- **Seleccionar las medidas que se implementarán (comparación de coste vs. beneficio).**
- **Estimar el nivel de riesgo residual.**
- **Adoptar las medidas según sean:**
  - **Medidas proactivas (preventivas).**
  - **Medidas reactivas (continuidad y recuperación).**
  - **Aceptar el riesgo residual si se cumplen los criterios de aceptación (no hacer nada).**
- **Evaluar la efectividad de las medidas (vulnerabilidades corregidas, amenazas evitadas en impacto y/ o frecuencia), para volver a iniciar el AR.**



Actividades

PROPONGA SOLUCIONES QUE MITIGUEN, EVITEN, O TRANSFIERAN LOS RIESGOS DE INUNDACIÓN, CORTE DE SUMINISTRO ELÉCTRICO, ROBO DE INFORMACIÓN POR BOICOT INTERNO, Y ERROR LÓGICO DE UNA APLICACIÓN DE CONTABILIDAD INTERNA.