SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

2.3.0.MF0487_3. Capítulo 3
Parte 2 de 2

Análisis de riesgos de los sistemas de información

JOSÉ PABLO HERNÁNDEZ

10. OPTIMIZACIÓN DEL PROCESO DE AUDITORÍA

Con la corrección de las vulnerabilidades detectadas y la continua evaluación de los sistemas de información, debe producirse un proceso de aprendizaje que deberá reflejarse en el informe de auditoría, permitiendo así una optimización constante y progresiva del proceso de auditoría.

10.1. EL INFORME DE AUDITORÍA

El informe de auditoría es un documento formalizado que contiene los objetivos de la auditoría, las metodologías utilizadas, los resultados obtenidos y las conclusiones y recomendaciones aportadas por los auditores.

Este informe tiene que ser claro, conciso, oportuno, objetivo e imparcial y debe ser elaborado por auditores independientes.

10.1. EL INFORME DE AUDITORÍA

En cuanto a la gestión de riesgos, el informe de auditoría deberá contener también los activos de la organización y su valoración, junto con las vulnerabilidades, amenazas y riesgos detectados en el sistema de información detectado.

Además, deberán formularse recomendaciones de políticas y medidas correctivas que permitan la reducción del riesgo y de posibles vulnerabilidades, además de proponer salvaguardas que reduzcan la incidencia de vulnerabilidades.

11. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES

Las medidas de salvaguarda o de seguridad son medidas cuya función fundamental es reducir o eliminar un riesgo de dos formas:

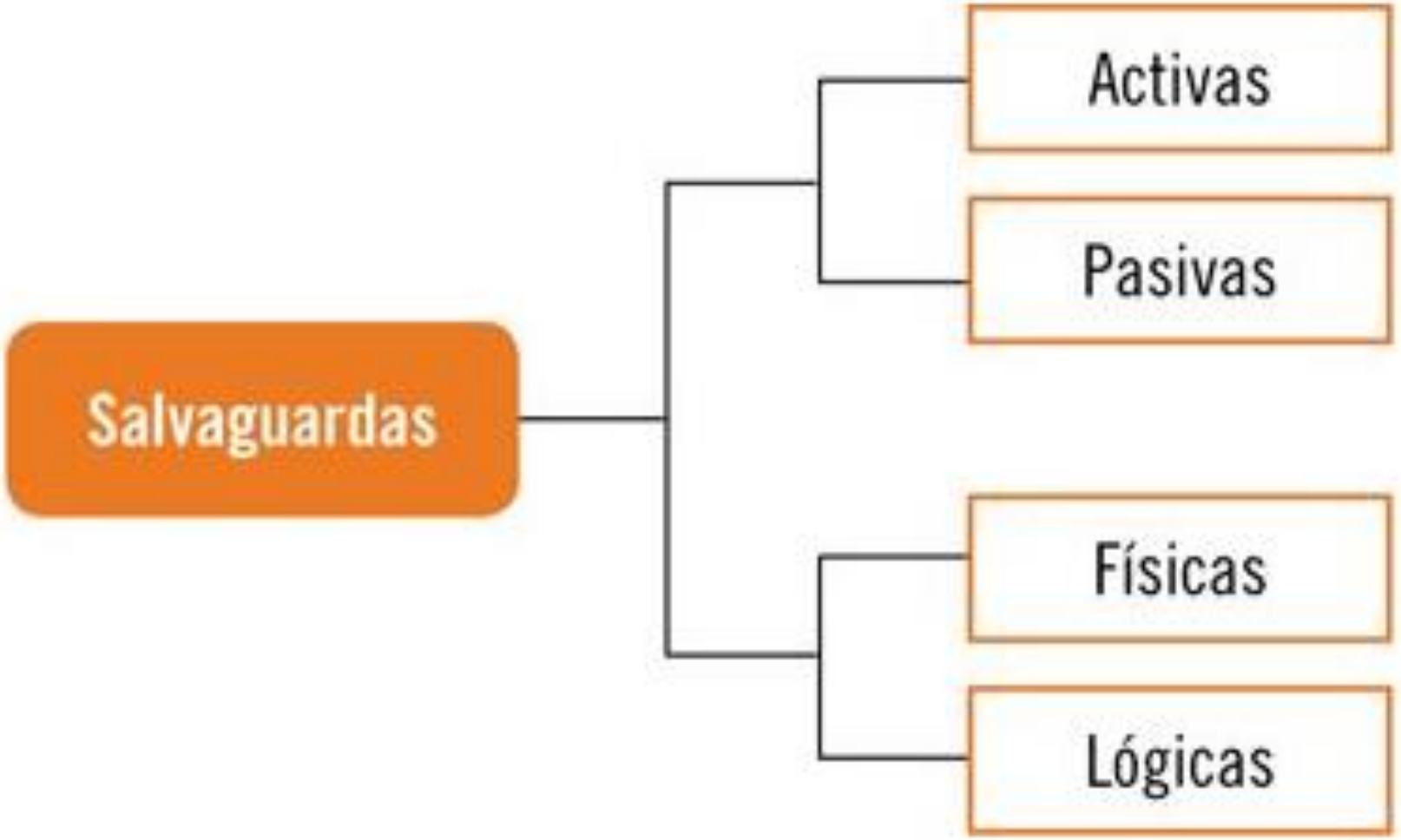
- **La reducción de la probabilidad de materialización de las amenazas:** son también salvaguardas preventivas.
- **La reducción del impacto de las amenazas:** hay salvaguardas que limitan o reducen la degradación del activo ante la presencia de alguna amenaza, impidiendo que el daño ocasionado se expanda.

11. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES

Las medidas de salvaguarda o de seguridad son medidas cuya función fundamental es reducir o eliminar un riesgo de dos formas:

- **La reducción de la probabilidad de materialización de las amenazas:** son también salvaguardas preventivas.
- **La reducción del impacto de las amenazas:** hay salvaguardas que limitan o reducen la degradación del activo ante la presencia de alguna amenaza, impidiendo que el daño ocasionado se expanda.

11. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES



11. IDENTIFICACIÓN DE LAS MEDIDAS DE SALVAGUARDA EXISTENTES

Salvaguarda ideal:

- Su implantación, configuración y mantenimiento deben ser perfectos.
- Debe emplearse en todo momento.
- Su protocolo de uso normal debe ser claro y, en caso de ocurrir cualquier incidencia, el personal debe estar correctamente formado para reaccionar de un modo rápido y eficaz.
- Deben estar implantados una serie de controles que avisen cuando se detecte cualquier tipo de fallo.

11.1. LAS SALVAGUARDAS Y LOS ACTIVOS

Cuando se implantan salvaguardas que forman parte del activo, hay que realizar un nuevo análisis de riesgos con el nuevo sistema desplegado para asegurarse de que el riesgo al que se expone el sistema es inferior a aquel al que estaba expuesto antes de implantarse la salvaguarda.

12. ESCENARIOS DE RIESGO: PARES ACTIVO-AMENAZA

- Estimar el impacto potencial al que se somete el sistema de información.

- Estimar el impacto residual al que se somete el sistema de información.

12.1. ESTIMACIÓN DEL IMPACTO POTENCIAL

Cálculo del escenario activo-amenaza:

- Activos identificados y su valoración.
- Amenazas identificadas y su valoración.

12.1. ESTIMACIÓN DEL IMPACTO POTENCIAL

IMPACTO		Degradación del activo		
		Inferior al 1 %	1-10 %	Superior al 10 %
Valor del activo	Muy alto	MEDIO	ALTO	MUY ALTO
	Alto	BAJO	MEDIO	ALTO
	Medio	MUY BAJO	BAJO	MEDIO
	Bajo	MUY BAJO	MUY BAJO	BAJO
	Muy bajo	MUY BAJO	MUY BAJO	MUY BAJO

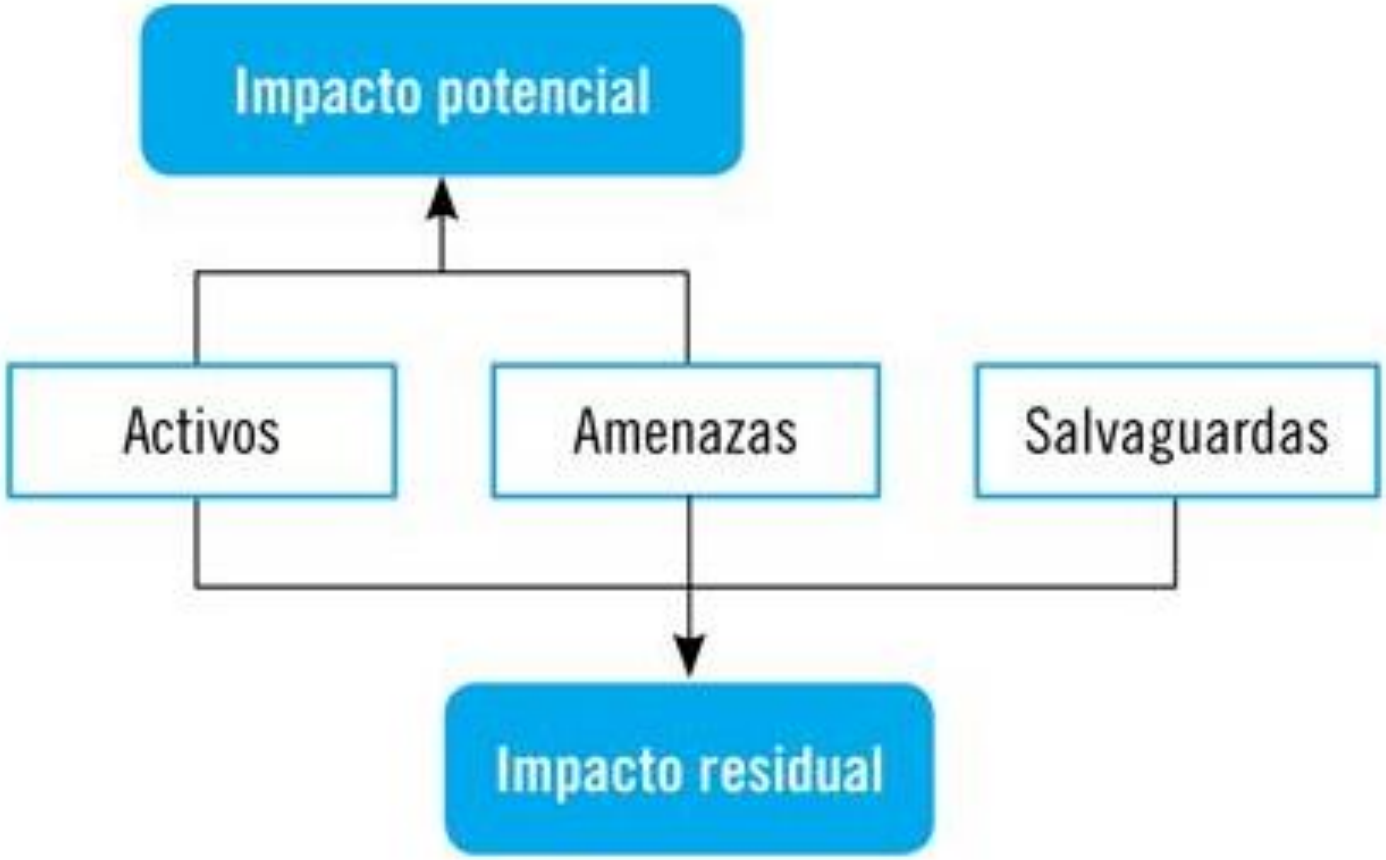
Ejemplo. Solución.

EL GRADO DE DEGRADACIÓN ES EL MISMO EN AMBAS EMPRESAS, POR LO QUE NO INFLUYE EN LA DIFERENCIA DE IMPACTO DE CADA UNA DE ELLAS.

SIN EMBARGO, AL INCLUIR INFORMACIÓN DE MAYOR VALOR EL EQUIPO DE LA EMPRESA A, SE CONSIDERA QUE TIENE UN MAYOR VALOR QUE EN LA EMPRESA B.

DE ESTE MODO, CON EL MISMO GRADO DE DEGRADACIÓN Y UN VALOR MAYOR PARA EL MISMO ACTIVO EN A QUE EN B, EL EQUIPO DE LA EMPRESA A SERÁ EL QUE SUFRA MÁS IMPACTO EN CASO DE MATERIALIZARSE ALGÚN TIPO DE AMENAZA QUE LE PUEDA AFECTAR.

12.2. ESTIMACIÓN DEL IMPACTO RESIDUAL



13. DETERMINACIÓN DE LA PROBABILIDAD E IMPACTO

Para establecer el nivel de riesgo de cada par de activo/amenaza, previamente hay que determinar la probabilidad y el impacto de materialización de los escenarios.

13.1. PROBABILIDAD DE MATERIALIZACIÓN DE LOS ESCENARIOS DE RIESGO

PROBABILIDAD	ESCALA	DESCRIPCIÓN	CALIFICACIÓN
Raro	0-20 %	Eventualidad casi nula	1
Improbable	20-40 %	Solo ocurre en ocasiones excepcionales	2
Probable	40-60 %	Puede ocurrir o no ocurrir	3
Altamente probable	60-80 %	Puede ocurrir bastantes veces	4
Casi certeza	80-100 %	Casi siempre ocurre	5

13.2. IMPACTO DE MATERIALIZACIÓN DE LOS ESCENARIOS DE RIESGO

IMPACTO	DESCRIPCIÓN	CALIFICACIÓN
Muy bajo	Impacto insignificante.	1
Bajo	Efectos mínimos para la organización.	2
Medio	Efectos considerables sobre los activos.	3
Alto	Efectos muy considerables para la organización en general.	4
Muy alto	Efectos irreparables o difícilmente reparables para la organización.	5

14. ESTABLECIMIENTO DEL NIVEL DE RIESGO PARA LOS DISTINTOS PARES DE ACTIVO Y AMENAZA

Los datos de entrada que se deberán utilizar para la estimación del riesgo serán los siguientes:

- Identificación y valoración de los activos.
- Identificación y valoración de las amenazas.
- Identificación y valoración de las salvaguardas.
- Impacto estimado con los pares activo/amenaza identificados.

14.1. NIVEL DE RIESGO DE LOS ESCENARIOS DE LOS PARES ACTIVO/AMENAZA

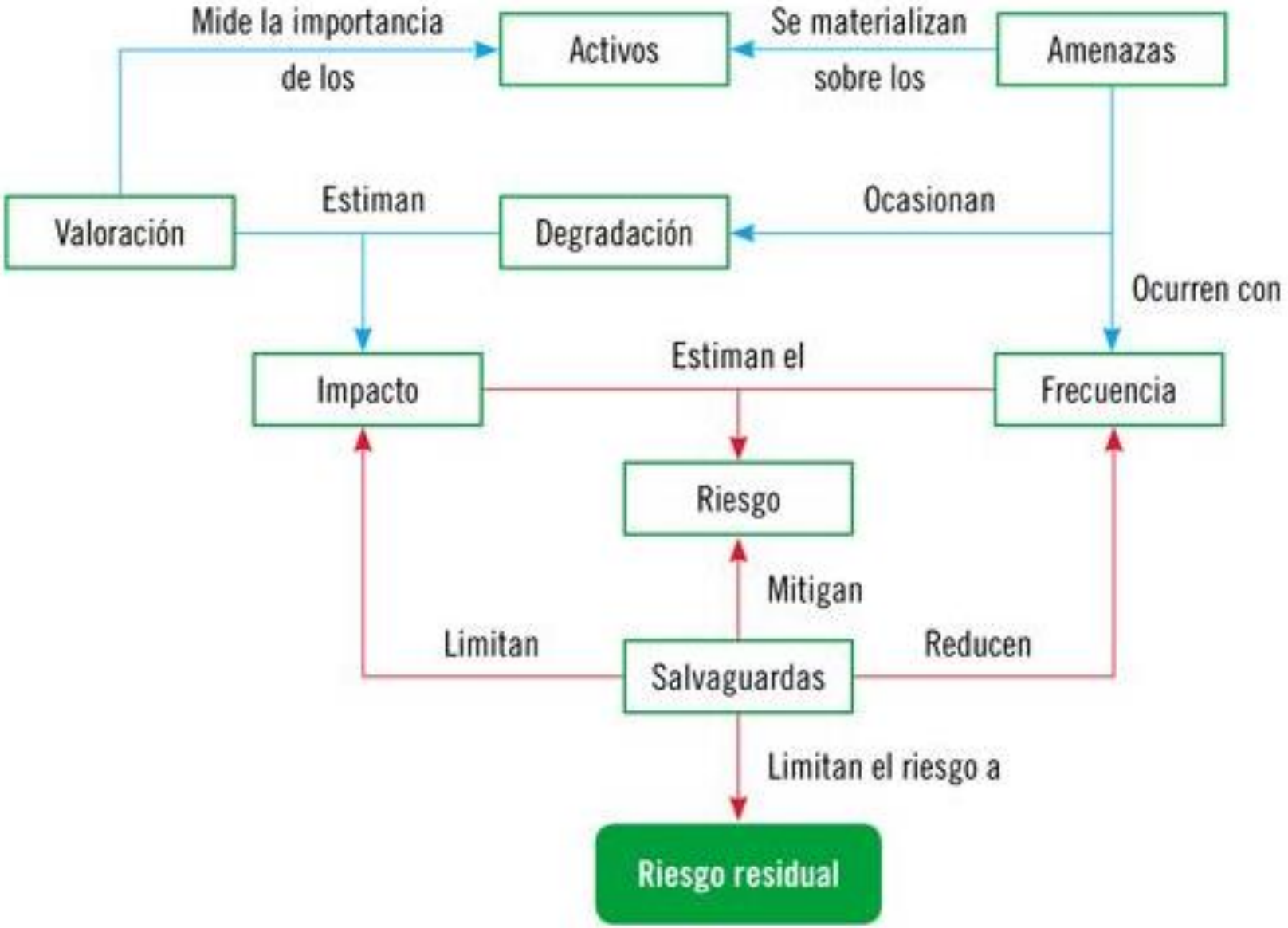
RIESGO = IMPACTO x PROBABILIDAD

15. DETERMINACIÓN DE LOS CRITERIOS DE EVALUACIÓN DEL RIESGO

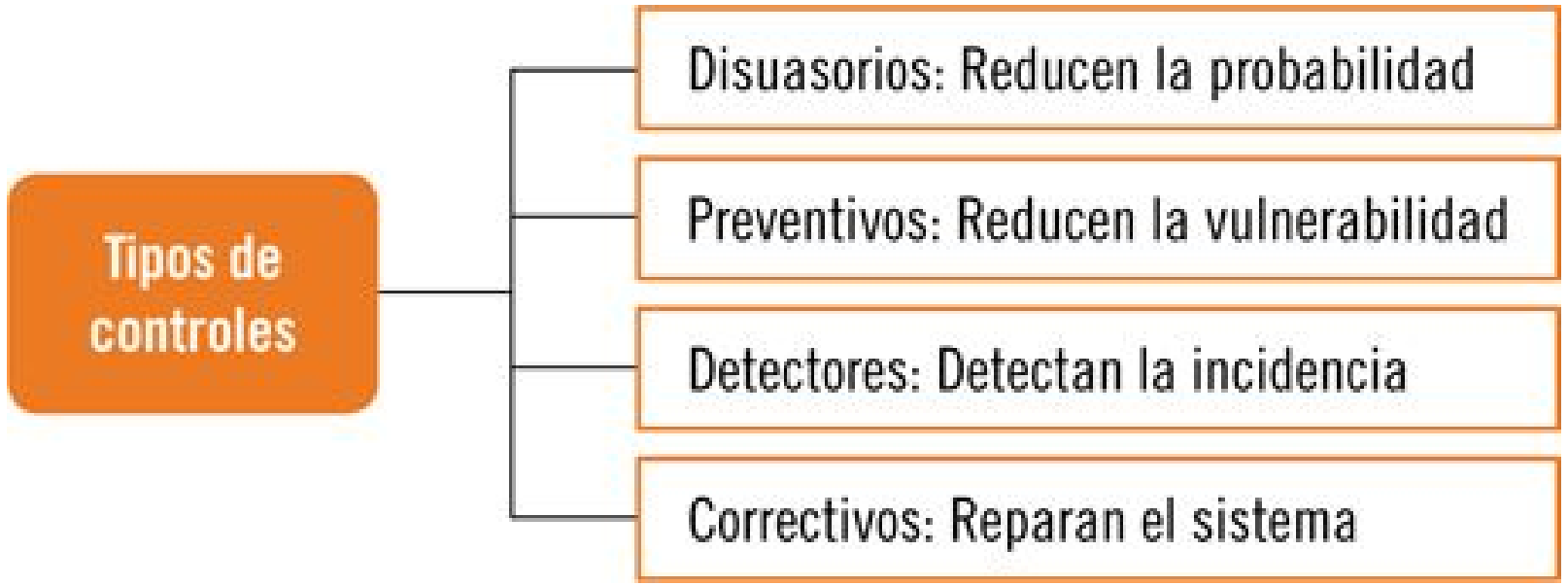
Con la evaluación de cada riesgo por separado, la organización obtendrá información valiosa que le permitirá:

- Establecer la probabilidad de materialización de amenazas.
- Calcular y estimar el impacto de las amenazas.
- Establecer criterios de valoración, calificación y evaluación de los riesgos.

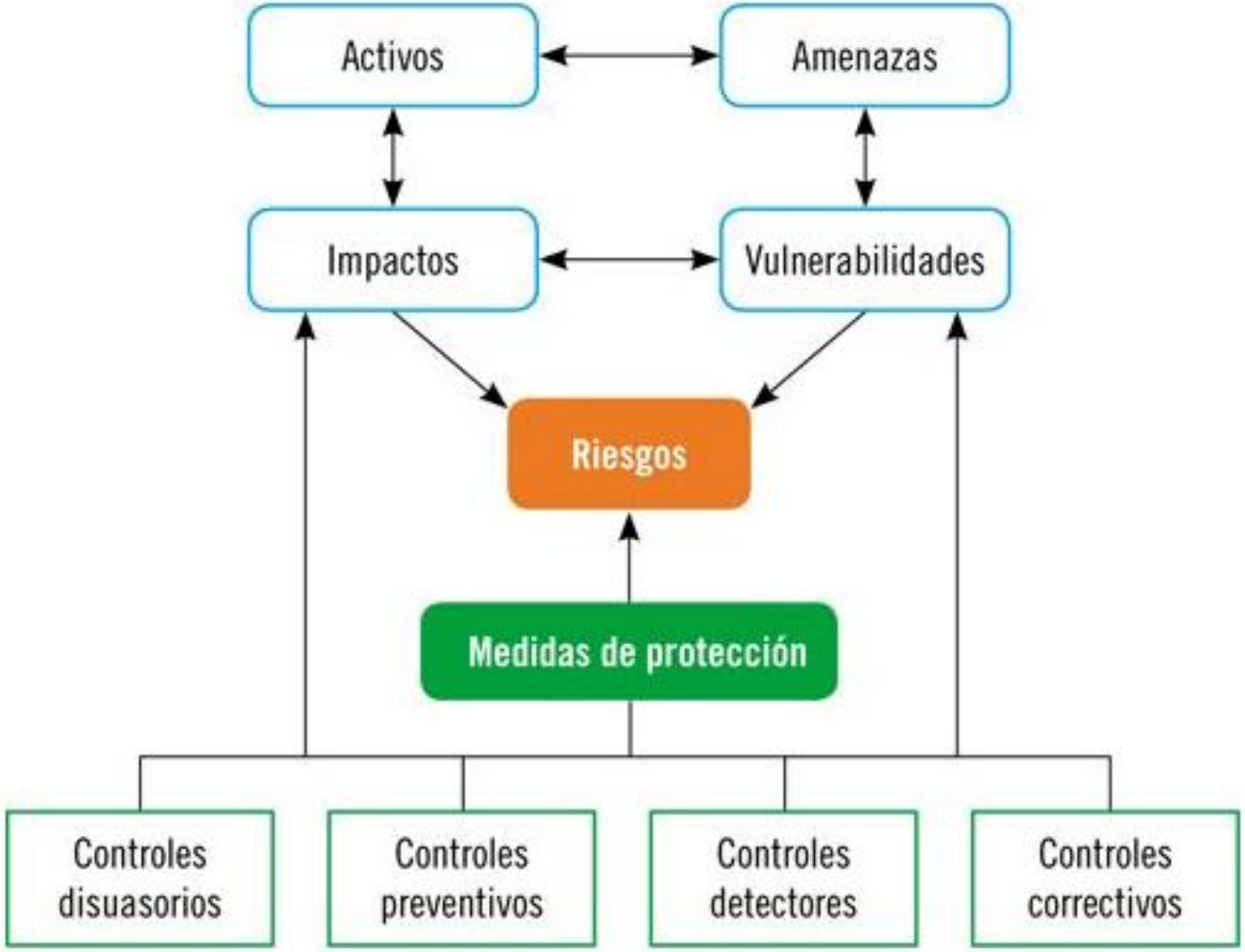
15.1. VISIÓN GENERAL DE LA GESTIÓN DE RIESGOS



16. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS



16. RELACIÓN DE LAS DISTINTAS ALTERNATIVAS DE GESTIÓN DE RIESGOS



17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

1. Conocer y entender el funcionamiento de la administración de riesgos

Amenaza: ¿qué puede suceder?

Probabilidad: ¿qué posibilidades hay de que suceda? ¿Con qué frecuencia?

Impacto: ¿qué efectos perjudiciales puede ocasionar la amenaza si se materializa?

Activo: ¿qué recursos pueden verse afectados?

Salvaguarda: ¿cómo puede reducirse el riesgo?

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

2. Definir las acciones del plan de gestión de riesgos

Deben establecerse acciones como los activos que se quieren evaluar, las posibles amenazas que se pueden materializar, qué metodología se va a utilizar, cuáles serán los umbrales de riesgo aceptables, etc.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

3. Conseguir el apoyo de la dirección y de profesionales externos

En casos en los que la reducción o eliminación del riesgo conlleva un coste elevado, se recomienda recurrir a profesionales externos que permitan la gestión del riesgo con menores costes y delegación de responsabilidades.

Por otro lado, los encargados de la gestión de riesgos deben contar con el apoyo de la dirección para que la actuación sea acorde con la misión global de la dirección y se integre como una actividad de esta.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

4. Identificar las consecuencias de cada riesgo

Teniendo en cuenta que cada riesgo conlleva consecuencias con perjuicios distintos, deben poder identificarse y valorar para conocer qué riesgos es necesario priorizar y atajar con más inmediatez.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

5. Eliminar las amenazas irrelevantes

Deberán descartarse aquellas amenazas cuyo impacto y probabilidad de ocurrencia sean mínimos para concentrar los recursos y esfuerzos en amenazas que puedan afectar a activos de alto valor, con la elaboración de un plan de contingencia.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

6. Inventariar los activos susceptibles de riesgo

Para tener controlados los riesgos, se recomienda tener un inventario de todos los activos de valor susceptibles de sufrir alguna amenaza. El inventario deberá actualizarse con cierta periodicidad.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

7. Asignar probabilidades

Para cada activo, deberán asignarse las probabilidades de materialización de cada activo y la frecuencia con la que se pueden producir.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

8. Asignar el impacto

Una vez asignadas las probabilidades, hay que asignar el grado de degradación que sufriría cada activo en caso de producirse la amenaza.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

9. Determinar el riesgo para cada activo

Con las probabilidades y los impactos estimados para cada activo, deberá calcularse una combinación de ambos factores para estimar el riesgo potencial de cada activo.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

10. Clasificar los riesgos

Con los riesgos calculados para cada activo, deberá elaborase una lista con todos ellos siguiendo un orden de prioridad de actuación: a mayor riesgo, mayor prioridad de actuación y viceversa.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

11. Calcular el riesgo total

Se calculará el riesgo total del sistema de información de la organización haciendo un promedio aritmético de todos los riesgos calculados de cada activo.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

12. Diseñar estrategias de reducción de riesgos

Para reducir el riesgo global de la organización, deberán tomarse decisiones de actuación sobre qué tipos de controles se pueden implantar y qué efectos pueden tener sobre los riesgos de la organización.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

13. Desarrollar planes de contingencia

Para los riesgos más importantes (que afectan a activos más valiosos y ocurren con más frecuencia) deberá diseñarse un plan de contingencia que permita reducirlos en el menor tiempo posible y restituir la situación previa, evitando que los daños ocasionados se expandan.

17. GUÍA PARA LA ELABORACIÓN DEL PLAN DE GESTIÓN DE RIESGOS

Recomendaciones básicas para la elaboración del plan

14. Analizar la efectividad de las estrategias implantadas

Si los riesgos no se han reducido o la reducción ha sido mínima, significará que las medidas implantadas no son eficaces y será necesaria una nueva evaluación para detectar en qué fallan y cómo pueden solucionarse.

Por el contrario, si se consigue reducir aceptablemente el riesgo, significará que los controles y salvaguardas son los correctos y que la gestión de riesgos se está llevando a cabo de un modo adecuado.

Ejercicios

2.3.100.1.MF0487_3_EJERCICIOSCAPITULO_3.DOCX