1.3.2.MF0486_3 - Capítulo 3 - Ejemplo

Para el cálculo de riesgo de un servicio, se tomará el ejemplo de un servicio de “cálculo de nóminas”, con valoración (CIA = muy alto, muy alto, bajo), formado por los activos: nóminas, aplicación de cálculo de nóminas, servidor, electricidad, y asesor Laboral.

El valor que estos activos tienen aislados no es relevante frente al del servicio, y se considera que las degradaciones se acumulan.

Por su frecuencia, se desea realizar una primera aproximación al análisis de riesgos para la amenaza de errores de configuración (el servidor se detiene una vez al mes, y es necesario reiniciarlo para que opere).

Por la degradación, se quiere analizar la amenaza de divulgación de la información (supondría un daño máximo, por la pérdida de confianza de los clientes, aunque su frecuencia es “muy poco frecuente”, por tratarse de ataques muy aislados, que suceden una vez cada varios años).

Determinar el riesgo del servicio, justificando las valoraciones que se estime oportuno realizar.

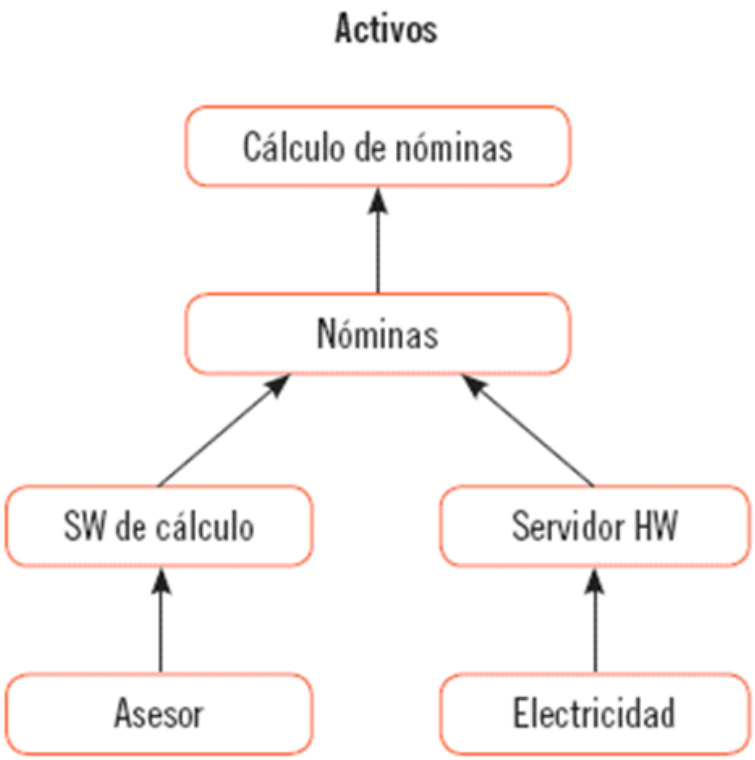
SOLUCIÓN

Se aplicará MAGERIT, en la fase 1, de análisis de riesgos.

Fase 1. Paso: 1 activos.

La jerarquía de los activos y su valor se conoce por el enunciado, y es el del servicio para todos los activos, porque estos por sí solos no aportan valor relevante.

Todos los activos valen: (5, 5, 2)



C	I	A
5	5	2

Valor	
MA	5
A	4
M	3
B	2
MB	1

Fase 1. Paso 2: amenazas.

Amenaza 1: Error de configuración.

Se trata de un error no intencionado, que de acuerdo al catálogo de MAGERIT, afecta al servicio, a las nóminas, al software de cálculo, y al servidor, de mayor a menor relevancia en las dimensiones: disponibilidad, integridad y confidencialidad.

La degradación que produce es parcial (el sistema se recupera reiniciando, y no se ha destacado otra información adicional), lo que se valora según las tablas vistas en el 10 %. Según la tabla de amenazas MAGERIT, las dimensiones se ven afectadas en orden C = 3, I = 2, A = 1; considerando que cada dimensión se ve afectada en la mitad que su anterior más prioritaria, la degradación CIA sería (2.5 %, 5 %, 10 %).

La frecuencia con que aparece es frecuente (el servicio se detiene 1 vez al mes), e igual en todas las dimensiones: 10

Amenaza 2: divulgación de la información.

Se trata de un error intencionado, que solo afecta a las nóminas en su confidencialidad.

La degradación que produce es completa (tratándose de un ataque intencionado, se considera que la cantidad y calidad de la información sustraída es total, o muy relevante), pero solo en la dimensión C, por lo que la degradación será: (100 %, 0 %, 0 %).

La frecuencia con que aparece, según el enunciado, es muy poco frecuente, lo que se valora según las tablas vistas en 1/ 10.

Fase 1. Paso 4: impacto.

El impacto se calcula para cada activo, para cada amenaza, y en cada dimensión, como el producto “Valor x Degradación”, obteniendo la siguiente tabla de valores:

Activo V = (5,5,2)	Amenaza 1: error configuración			Amenaza 2: divulgación		
	C (2.5 %)	I (5 %)	A (10 %)	C (100 %)	I (0 %)	A (0 %)
Servicio	0.125	0.25	0.2	-	-	-
Nóminas	0.125	0.25	0.2	5	0	0
Software	0.125	0.25	0.2	-	-	-
Hardware	0.125	0.25	0.2	-	-	-
Asesor	-	-	-	-	-	-

Por ejemplo: para el servicio, el valor en C es 5, y la degradación en C es del 2.5 %; por lo tanto, el impacto en C es el 2.5 % de 5, es decir 0,125.

Se calcula el impacto repercutido sobre el servicio, consecuencia del valor propio del activo, y de las amenazas a que están expuestos sus activos inferiores.

Como se indica en el enunciado, el criterio es el de sumar las degradaciones de los activos dependientes (aunque bien podría haberse indicado otro, como usar la degradación máxima), obteniéndose un impacto repercutido:

Activo V = (5,5,2)	Amenaza 1: error configuración			Amenaza 2: divulgación		
	C (7,5 %)	I (15 %)	A (30 %)	C (100 %)	I (0 %)	A (0 %)
Servicio	0.375	0.75	0.6	5	-	-

Fase 2. Paso 5: riesgo.

El riesgo total sobre el servicio será el riesgo repercutido, derivado del impacto repercutido sobre el servicio, y la frecuencia de las amenazas:

Activo V = (5,5,2)	Amenaza 1: error configuración			Amenaza 2: divulgación		
	C(10)	I (10)	A (10)	C (0.1)	I (0.1)	A (0.1)
Servicio	3.75	7.5	6	0.5	-	-

Al emplear tasas anuales para la frecuencia, los riesgos que se obtienen deben interpretarse como riesgos anuales, o pérdidas probables en un año.

En el ejemplo, para la integridad (7.5), y la disponibilidad (6), a lo largo del año se esperan pérdidas superiores al propio valor máximo del activo en esas dimensiones (5 y 2 respectivamente).

Esto es así, debido a la elevada tasa de ocurrencia de la amenaza que, siendo mensual, multiplica el impacto por 10 (aunque realmente debiera multiplicarse por 12, que es el número de ocurrencias en el año, esta diferencia no es relevante: lo importante realmente es emplear siempre el mismo criterio para comparar).

Se suman ahora los valores de las dos amenazas:

Activo V = (5,5,2)	Amenazas 1 y 2: error configuración y divulgación		
	C	I	A
Servicio	4.25	7.5	6

Pese a que dimensiones diferentes obedecen a propiedades de la información diferentes, MAGERIT permite agregarlas, dando como valor último del riesgo: 17.75. Si el valor del servicio es 12 (C + I + A), las pérdidas probables esperadas en un año por las amenazas estudiadas son de 17.75, es decir, del 148 % de la valoración del activo en seguridad de la información (empleando muy alto = 5, alto = 4, medio = 3, bajo = 2, muy bajo = 1). Aunque resulta difícil no hacer una interpretación del valor anterior, es importante recordar que, por sí solo, este dato no tiene ningún significado. El único significado procederá de la comparación frente a otro riesgo calculado de la misma manera, es decir, con un criterio homogéneo. Por ejemplo, frente a otro servicio de la empresa, o frente al mismo servicio después de aplicar salvaguardas.