¿Cómo se mide la gestión de riesgos?

RESUMEN: Para poder hacer una buena gestión del riesgo, hay que hacer un análisis dividiéndolo en una serie de fases.

CATEGORÍAS: CIBERSEGURIDAD

Nº HIPERVINCULOS: 1

La gestión de riesgos está presente, en mayor o menos medida, en diferentes ámbitos; uno de ellos es en la **seguridad de la información.** Para poder medir la gestión del riesgo, hay que dividirlo en las siguientes fases según señala INCIBE:

1. **ALCANCE.** El primer paso a la hora de llevar a cabo el análisis de riesgos, es establecer el alcance del estudio. Vamos a considerar que este análisis de riesgos forma parte del Plan Director de Seguridad (PDS). Por lo tanto, recomendamos que el análisis de riesgos cubra la totalidad del alcance del PDS, dónde se han seleccionado las áreas estratégicas sobre las que mejorar la seguridad. Por otra parte, también es posible definir un alcance más limitado atendiendo a departamentos, procesos o sistemas.
2. **IDENTIFICAR LOS ACTIVOS.** Hay que identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio.
3. **DETECTAR LAS AMENAZAS.** El conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado.
4. **IDENTIFICAR LAS VULNERABILIDADES.** Observar cuáles son las características de nuestros activos para identificar puntos débiles o vulnerabilidades. Por ejemplo, una posible vulnerabilidad puede ser identificar un conjunto de ordenadores o servidores cuyo sistema antivirus no están actualizados o una serie de activos para los que no existe soporte ni mantenimiento por parte del fabricante. Posteriormente, a la hora de evaluar el riesgo aplicaremos penalizaciones para reflejar las vulnerabilidades identificadas.
5. **EVALUAR EL RIESGO.** Se realiza de manera que para cada par activo-amenaza, estimaremos la probabilidad de que la amenaza se materialice y el impacto sobre el negocio que esto produciría. El cálculo de riesgo se puede realizar usando tanto criterios cuantitativos como cualitativos.
6. **TRATAR EL RIESGO.** Siguiendo las siguientes 4 estrategias:
   - **Transferir el riesgo a un tercero.** Por ejemplo, contratando un seguro que cubra los daños a terceros ocasionados por fugas de información.
   - **Eliminar el riesgo.** Por ejemplo, eliminando un proceso o sistema que está sujeto a un riesgo elevado.
   - **Asumir el riesgo, siempre justificadamente.** Por ejemplo, el coste de instalar un grupo electrógeno puede ser demasiado alto y por tanto, la organización puede optar por asumir.
   - **Implantar medidas para mitigarlo.** Por ejemplo, contratando un acceso a Internet de respaldo para poder acceder a los servicios en la nube en caso de que la línea principal haya caído.

Por último, cabe señalar que como realizamos este análisis de riesgos en el contexto de un PDS, las acciones e iniciativas para tratar los riesgos pasarán a formar parte del mismo. Por lo tanto, deberemos clasificarlas y priorizarlas considerando el resto de proyectos que forman parte del PDS.