PRINCIPIOS Y BUENAS PRÁCTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

PEC1

Álvaro Pérez Rey
Normativa en ciberseguridad

Índice

1. Ejercicio A

A.1. Pon un ejemplo de cada uno de los pilares básicos de la seguridad informática, explícalo detalladamente.

- Confidencialidad: A la hora de acceder a los archivos pertenecientes a un departamento en concreto, un ejemplo sería que exclusivamente los trabajadores del departamento de contabilidad tengan acceso a las nóminas de los trabajadores de la empresa.

- Integridad: Comparar los hashes de un disco duro y la copia de este, si el hash es diferente este disco estaría modificado y no guardaría la integridad del mismo.

- Disponibilidad: En el caso de los servidores en redundancia ya que garantiza en mayor medida el acceso a esa información.

- Autenticidad: Un ejemplo claro sería la firma electrónica o la firma digital.

- Fiabilidad: En el caso de los backups, que estos sean totalmente usables y no dispongan de ninguna avería o si estos backups se están haciendo de forma errónea.

- No repudio: También se puede utilizar el ejemplo de la firma digital ya que existe una evidencia clara de que el individuo/a ha realizado dicha acción.

- Responsabilidad: El control exhaustivo del tratamiento de información dentro de una empresa, es decir, los pasos tales como la confidencialidad en sí, por ejemplo, es un ejemplo de que las empresas deben tener un control y un cuidado de estos datos ya que es responsabilidad de la misma compañía.

2. Ejercicio B

B.1. Busca información en Internet sobre metodologías de gestión de riesgos que no estén basadas en activos. Destaca las principales características y describe brevemente el proceso.

Metodología general de evaluación de riesgos.

Esta metodología permite cuantificar la magnitud de los distintos riesgos de accidente existentes en un lugar o puesto de trabajo, lo que conduce al establecimiento razonado de un plan de actuación en el que se fijen las prioridades en función de la magnitud del riesgo obtenida.

El método parte de la detección de las deficiencias en materia de prevención existentes en el lugar/puesto de trabajo. Detectada la deficiencia, se estima la probabilidad de que ocurra un accidente, y teniendo en cuenta la magnitud de las posibles consecuencias esperadas, se procede a la evaluación del nivel de riesgo derivado de la deficiencia existente.

Así pues, se consideran cuatro factores:

1. Nivel de deficiencia.
2. Nivel de exposición.
3. Nivel de probabilidad.
4. Nivel de consecuencias.

A cada uno de los factores se les asigna un valor numérico que, una vez realizados los cálculos necesarios, nos permite la cuantificación del nivel de riesgo alcanzado, a partir del cual se establece el nivel de intervención que se tiene que realizar.

Se trata de una metodología simple de aplicar y que se obtienen unos resultados muy ajustados a la realidad, al contemplar aspectos globales que en otras metodologías pasan desapercibidos.

Tiene una aplicación generalizada, por lo tanto, es aplicable en cualquier actividad o en edificios de cualquier naturaleza, pudiendo decir que se trata de una metodología de empleo universal.

Igualmente hay que reseñar que es una metodología recomendada por el INSHT (Instituto Nacional de Seguridad e Higiene en el Trabajo) y adoptada a nivel institucional en la evaluación de riesgos organizacionales, así como por la Unidad Militar de Emergencias y otros Cuerpos de Seguridad del Estado.

FMEA (Failure Mode and Effective Analysis)

Esta **metodología de gestión de riesgos** es en realidad una técnica de ingeniería. En principio fue creada por la Nasa, pero después fue adoptada en diferentes campos e industrias. El método FMEA consiste en identificar, clasificar y eliminar las fallas de los proyectos o de los procesos antes de que estas ocurran.

El método FMEA empieza identificando las posibles fallas y efectos. Posteriormente, se crea una clasificación de ellos. La puntuación de los riesgos se determina teniendo en cuenta tres criterios:

1. Frecuencia.

2. Gravedad.

3. Detección.

Con esos tres puntos se aplica una fórmula que permite establecer cuáles fallas son más o menos graves. Los riesgos más críticos deben ser atendidos primero que los demás.

3. Ejercicio C

C.1. En esta ocasión hablaremos sobre la gestión de riesgos, que se puede dividir principalmente en 3 etapas:

- Análisis de riesgos.
- Tratamientos de riesgos.
- Plan de tratamiento de riesgos.

Hasta aquí todo bien, pero:

- **¿Qué es realmente un activo?:** Es un recurso con valor que alguien o algo posee con la intención de que genere beneficio, económico o no, en un futuro. Representa los bienes y derechos de una empresa.

- **¿Un activo puede ser una consola de aire acondicionado?**: En efecto, puede serlo o no, esto depende del fin que tenga este aire acondicionado, es decir, si su función es meramente para regular la temperatura de la zona de trabajadores quizás no requiera contarlo como un activo pero si su función, digamos, es mantener una temperatura adecuada en la sala donde se encuentran los servidores para que así estos no se calienten y pueda dar fallos de temperatura si podríamos considerarlo un activo y bastante importante.

  En resumen, podremos considerar algo/alguien un activo en función del impacto que tenga o consideren que tenga.

- **¿En la ISO 27001 es obligatorio el uso de activos?:** Es obligatorio que se adjunte información documentada acerca de **Inventario de activos (8.1.1)** y **Reglas para el uso aceptable de activos (8.1.3)** por lo que reconocemos como obligatorio el uso de activos.

- **¿Podríamos evaluar riesgos sin basarnos en activos?:** Claro, como hemos visto en apartados anteriores hay opciones para la evaluación de riesgos sin basarnos en activos como el uso de una metodología de evaluación de riesgos de manera general que evalúa 4 apartados como son: deficiencia, exposición, probabilidad y consecuencias.

  Aunque también hay muchos más otro ejemplo sería FMEA, aunque se puede considerar una técnica de ingeniería, esta metodología empieza identificando las posibles fallas y efectos basadas en: frecuencia, gravedad y detección. Estos 3 apartados aplicados en una fórmula permiten estableces cuales fallas son más o menos graves.

4. Webgrafía

- https://www.piranirisk.com/es/blog/5-m%C3%A9todos-de-an%C3%A1lisis-de-riesgos
- https://www.urbicad.com/mico/metodos_riesgos.htm
- https://economipedia.com/definiciones/activo.html
- https://www.escuelaeuropeaexcelencia.com/2019/10/documentacion-en-iso-27001-obligatoria-y-no-obligatoria/