**MF0486\_3 : Unidad de Aprendizaje 4 - Ejercicios de Repaso y Autoevaluación**

**1. Empareje las siguientes términos, correspondientes a diferentes aspectos de cada fase de un SGSI:**

a. Establecimiento.

b. Monitorear y revisar.

c. Corregir.

d. Implementación y operación.

e. ¿Cómo modificar el rumbo?

f. Implantación de salvaguardas.

g. Planear.

h. ¿Dónde estamos?

**2. Si el nivel de seguridad CIA de un proceso es (4,5,1), y el nivel requerido es (1,8,1), el informe de insuficiencias concluirá que...**

a. ... el nivel de seguridad existente (4+5+1=10) cumple los requerimientos de seguridad de la empresa (1+8+1=10).

b. ... hay un déficit de 3 puntos en la integridad existente (5) frente a la requerida (8). Por tanto, integridad no alcanzada, inferior a 8: 5.

c. ... debe invertirse en mejorar la integridad.

d. No se indicará nada, porque no se alcanzan los valores de riesgo máximo admisibles.

**3. Una fuente para los requisitos de seguridad de una empresa es:**

a. El resultado de una auditoría de seguridad del cumplimiento de la norma ISO 27001.

b. El presupuesto de seguridad.

c. Los principios, los objetivos, y los requerimientos comerciales que el sistema de información debe cumplir para sostener las operaciones de la empresa.

d. Un método de valoración CIA de un proceso, coincidente con la valoración CIA de su información crucial.

**4. Elija la secuencia temporal de intervención de los controles:**

a. Organizativos, prevención, de detección física, emergencia, y recuperación.

b. Primero los de detección, luego los de emergencia, luego los de recuperación, y por último, los de prevención, para evitar que se repitan.

c. Preventivos, correctivos, y adaptativos o perfectivos.

d. Preventivos, de detección, de emergencia, y de recuperación.

**5. Bajo unos criterios generales, elija que conjunto de salvaguardas resulta óptimo:**

a. Medidas físicas y técnicas, para la detección y recuperación, pero muy difíciles de operar.

b. Medidas preventivas, de detección y recuperación, organizativas y técnicas, de complejidad moderada, y con un programa de actualizaciones periódicas.

c. Una aplicación de detección y recuperación integrada, que se ejecuta sola, y apenas necesita intervención humana cuando se activa, pero sin actualizar ni revisar desde hace años.

d. Las más económicas que cumplan la legislación vigente.

**6. ¿A qué tipo de activo aplican las siguientes salvaguardas, según el método MAGERIT?**

**7. Según ISO 17779, e ISO 27002, los controles esenciales son los siguientes:**

a. La protección de datos y privacidad de la información, los derechos de propiedad intelectual, y la protección de los registros de la empresa.

b. El marco regulatorio, los objetivos organizacionales, los requerimientos y restricciones de operación, un costo de implementación en relación al riesgo que se reduce proporcional a los requisitos de la empresa, y el equilibrio entre coste de implementación y el riesgo.

c. 133 controles, agrupados en 39 objetivos de 11 dominios básicos.

d. No existen unos controles esenciales, porque dependen del sector de actividad de cada empresa.

**8. Indique qué controles deben incluirse en una declaración de aplicabilidad:**

Controles seleccionados, Controles existentes y Controles excluidos.

**9. Complete la siguiente frase:**

El Esquema Nacional de Seguridad establece la política de seguridad en la utilización de medios electrónicos, y está constituido por **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** y **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** para una adecuada SI.

**10. Indique a qué fase de un SGSI pertenecen las siguientes tareas:**

- Identificar los riesgos

- Tomar medidas preventivas y correctivas.

- Revisar evaluaciones de riesgo.

- Definir efectividad controles.

- Analizar y evaluar los riesgos.

- Plan de tratamiento de riesgos.

- Detección y respuesta a incidentes.

- Seleccionar controles para riesgos.

**11. Según ISO 27001, el plan de tratamiento de riesgos, debe identificar:**

**12. Los procesos de la norma ISO 27003, que dan pautas sobre la información que se debe recoger de cada control o salvaguarda, lo que resulta muy valioso para su implantación, son:**

a. La revisión del marco legislativo, las normas y requisitos operacionales, los principios, y objetivos (incluidos los comerciales) que debe cumplir el   
 sistema de información para sostener las operaciones de la empresa.

b. El análisis y gestión de riesgos, la elaboración de una declaración de aplicabilidad, y una auditoría que concluya en un informe de insuficiencias.

c. El diseño de contramedidas en la seguridad organizacional, y el diseño de contramedidas en seguridad física y de las TIC.

d. Los mismos que se marcan en la norma 17799:2005.

**13. Enumere el contenido recomendado para cada acción a ejecutar dentro del plan de tratamiento de riesgo, según las normas ISO 27000:**

**14. Enumere el contenido recomendado de cada programa de seguridad, según MAGERIT:**

**15. A la vista de las siguientes curvas de comparación de pérdidas y ganancias, elija la mejor opción:**