**RUNE BRITO NUÑEZ**

**SEGURIDAD INFORMATICA**

**MF0486\_4. UD4 – RESPUESTAS:**

**1. Empareje los 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?**

\*Registro de intrusiones. 🡪 (Equipos)

\*Control de acceso de las entradas/salidas de personas y equipos. 🡪 (Seguridad Física)

\*Protección frente a dañino (virus, troyanos, etc.). 🡪 Aplicaciones

**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 el código 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 principios básicos y requisitos mínimos

para una adecuada SI.

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

~**~** Identificar los riesgos. (Establecer SGSI)

~**~** Tomar medidas preventivas y correctivas. (Mantener y mejorar SGSI)

~**~** Revisar evaluaciones de riesgo. (Monitorear y revisar SGSI)

~**~** Definir efectividad controles. (Implementar y operar SGSI)

~**~** Analizar y evaluar los riesgos. (Establecer SGSI)

~**~** Plan de tratamiento de riesgos. Implementar y operar SGSI

~**~** Detección y respuesta a incidentes. (Implementar y operar SGSI)

~**~** Seleccionar controles para riesgos. (Establecer SGSI)

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

Que identifique: La acción, los recursos , las responsabilidades, Las prioridades de la gerencia para manejar los riesgos y el ´SI`

**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:**

–– Descripción de la acción

–– Prioridad de riesgos de SI para gerencia, que apoya ejecutar la acción

–– Recursos necesarios para la acción

–– Consideraciones de financiación

–– Funciones y responsables en la ejecución de la acción

–– Medidas de eficacia de controles

–– Para cada control, aspectos del diseño de los controles para su

implantación:

–– Descripción detallada del control

–– Nombre de la persona responsable del diseño y la implantación

–– Prioridad de la implantación

–– Periodo de tiempo en que el control debe estar implantado

–– Tareas o actividades para implementar el control, detallados paso a paso

–– Recursos concretos para la implantación de este control

–– Persona a quien se debe informar que el control se ha implantado

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

• objetivo genérico

• prioridad o urgencia

• ubicación temporal: ¿cuándo se llevará a cabo?

• salvaguardas involucradas

• unidad responsable de su ejecución

• estimación de costes financieros

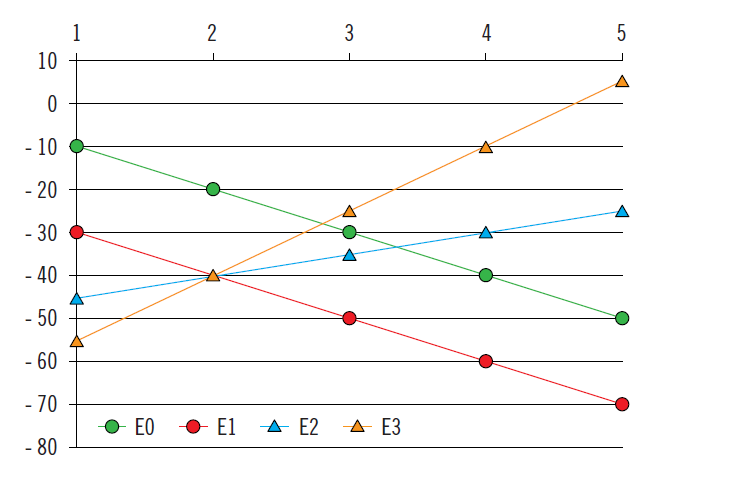
• estimación de recursos

• estimación de impacto para la organización

Fuente:>> [Libro II – Magerit - página 74](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

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

**mejor opción:**



El caso más óptimo es el E3. Ya que es el de mayor inversión inicial, se obtiene rentabilidad en

el año 3, e incluso se obtienen beneficios operativos en el año 5.