**RUNE BRITO NUÑEZ**

**SEGURIDAD INFORMATICA**

**MF0486-3. UD3. Ejercicios de repaso y autoevaluación**

**1. Complete la siguiente oración:**

Por simplicidad, el análisis y gestión de riesgos se suele acortar a gestión de riesgos, pero en ningún caso este nombre corto supone eliminar la etapa inicial de análisis de riesgos.

**2. Indique 2 situaciones en las que conviene realizar un AGR, y una en la que sea obligatorio:**

Conviene realizarlo cuando; la empresa dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión

Conviene realizarlo antes de emprender cambios profundos o realizar inversiones de renovación tecnológica

Será obligatorio para conducir una auditoría de seguridad, o definir el marco de cumplimiento de una ley

**3. Enumere las 4 decisiones que se pueden adoptar frente a los riesgos detectados:**

1. Requisitos legales
2. Requisitos operacionales
3. Objetivos de la empresa
4. Rentabilidad de la acción

**4. Marque la opción correcta:**

a. La decisión sobre qué hacer con los riesgos, vendrá dada exclusivamente por la rentabilidad de la acción, buscando el mínimo coste total.

b. En la decisión sobre qué hacer con los riesgos, los requisitos legales siempre deben cumplirse.

c**.** En la decisión sobre qué hacer con los riesgos, entre otros, pueden intervenir los requisitos legales, los requisitos operacionales, los objetivos de la   
 empresa, y la rentabilidad de la acción.

d. En la decisión sobre qué hacer con los riesgos, solo se tendrá en cuenta el riesgo residual alcanzado.

**5. Determine la opción que elegiría cuando un riesgo es despreciable, comparado con el criterio de aceptación de riesgos de la empresa:**

a. No hacer nada.

b. Mitigar el pequeño riesgo residual que presenta para lograr evitarlo.

c. Corresponde a la Dirección de la empresa autorizar la aceptación del riesgo.

d. Esperar a que el riesgo crezca para poder tratarlo convenientemente.

**6. Seleccione la afirmación más adecuada, acorde con el método MAGERIT:**

a. Conocer para asegurar: conocer los riesgos para poder afrontarlos y reducirlos.

b. Conocer para confiar: conocer los riesgos para poder afrontarlos y controlarlos.

c. Conocer para ocultar: esconda sus riesgos para reducir las amenazas.

d. Conocer para desconfiar: cuanto más se conoce el sistema, aparecen más vulnerabilidades.

**7. Determine los pasos habituales del análisis de riesgos en MAGERIT:**

a. Paso 1, paso 2, paso 4, paso 3, paso 5.

b. Paso 1, paso 2, paso 3, paso 4, paso 5.

c. Paso 1, paso 2, paso 4, paso 5, paso 3.

d. Paso 1, paso 2, paso 5, paso 3, paso 4.

**8. Complete la siguiente frase:**

El activo esencial es la información o datos, y alrededor se encuentran también otras familias de activos.

**9. Indique los nombres de las capas en que puede organizar los activos que contribuyen a la entrega de un servicio que emplea sistemas de información.**

Capa 4: las funciones y procesos de la organización (objetivos, bienes,

y servicios producidos).

Capa 3: la información y los datos.

Capa 2: el sistema de información propiamente dicho (aplicaciones,

equipos, soportes, equipamiento auxiliar, y redes de comunicaciones).

Capa 1: el entorno que se precisa (equipamiento y suministros eléctricos

de climatización y de comunicaciones, el personal, y otros,

como el edificio o el mobiliario).

**10. Indique si es verdadero o falso**

a. MAGERIT recoge todas las amenazas que puede enfrentar un SI:

Verdadero

 Falso

b. MAGERIT no incluye un catálogo de amenazas. En su lugar debe emplearse ISO 27002 y el buen juicio profesional del analista para determinar las   
 idóneas:

 Verdadero

Falso

c. MAGERIT incluye un conjunto de amenazas, agrupadas en 4 categorías, señalando las familias de activos habitualmente dañadas, y las   
 dimensiones que se verán dañadas de mayor a menor relevancia:

Verdadero

 Falso

**11. ¿Qué dato emplearía en MAGERIT para las siguientes valoraciones? Indique verdadero o falso:**

a. Una degradación de 0.1, si la amenaza daña parcialmente.

Verdadero

 Falso

b. Una frecuencia de 10, si ocurre una vez al año.

 Verdadero

Falso

c. Una degradación del 0.1 %, si la amenaza apenas daña el activo.

 Verdadero

 Falso

d. Una frecuencia de 100, si la amenaza sucede casi a diario.

Verdadero

 Falso

**12. Defina las siguientes magnitudes:**

a. El impacto repercutido . Suma de las degradaciones de los activos pendientes

b. El riesgo acumulado. Riesgo por impacto acumulado de un activo a raíz de la frecuencia de su amenaza

c. El impacto acumulado. Impacto sobre el valor acumulado de un activo , a raíz de su amenaza

d. El riesgo repercutido Riesgo total sobre el servicio

**13. Indique cuáles de las siguientes operaciones se pueden realizar al considerar una jerarquía de activos en un AGR:**

a. Puede agregar impactos (riesgos) de diferentes amenazas sobre un mismo activo.

 Verdadero

 Falso

b. Puede agregar impactos repercutidos sobre diferentes activos.

Verdadero

 Falso

c. Puede agregar riesgos acumulados sobre diferentes activos.

 Verdadero

 Falso

d. No puede agregar impactos (riesgos) en diferentes dimensiones.

Verdadero

 Falso

**14. Marque cuáles de las siguientes fórmulas son válidas:**

a. Riesgo residual = Impacto repercutido x frecuencia mejorada.

b. Impacto residual = Impacto x (100 – eficacia de la salvaguarda)

c. Riesgo residual = Impacto residual x frecuencia mejorada.

**15. Identifique las curvas de la siguiente imagen:**

Coste

(2)

(1)

Seguridad

1. Coste de riesgo residual
2. Coste de salvaguardas