**RUNE BRITO NUÑEZ**

**SEGURIDAD INFORMATICA**

**MF0486\_3. UD1 – RESPUESTAS:**

**1. De las siguientes frases, indique cuál es verdadera y cuál es falsa.**

a. Una amenaza es la probabilidad de que haya un fallo que dañe los sistemas.

 Verdadero

 Falso

b. Una amenaza es un posible hecho que dañaría los sistemas.

Verdadero

 Falso

c. Se puede eliminar una amenaza reduciendo su vulnerabilidad.

 Verdadero

 Falso

**2. Determine la fórmula correcta:**

a. Riesgo = amenaza + vulnerabilidad.

b. Riesgo = probabilidad x vulnerabilidad.

c. Riesgo = impacto x vulnerabilidad.

d. Riesgo = probabilidad x daño.

**3. Complete las siguientes definiciones:**

a. Disponibilidad es que la información esté disponible siempre que se necesite.

b. Confidencialidad es que la información solo esté accesible para quien esté autorizado a ello.

c. La Integridad es que la información sea válida, exacta, y completa.

d. Fiabilidad o seguridad, es que el comportamiento de un sistema sea predecible, según su diseño y construcción.

**4. Determine la combinación correcta de propiedades:**

a. Fiabilidad = confidencialidad + precisión + exactitud.

b. Seguridad = confianza + integridad + disponibilidad.

c. Seguridad = confidencialidad + integridad + disponibilidad.

**5. Complete la siguiente oración:**

Un modelo de seguridad orientado a la gestión de riesgos, persigue organizar la gestión de la seguridad en base a dos factores: un método para calcular riesgos delsistema de información\_ y unas \_directrices, basadas en estrategias empresariales y normativas

,

**6. Complete las siguientes definiciones:**

a. La gestión de riesgos permite la elección de unas salvaguardas u otras, según unas directrices empresariales.

b. El análisis de riesgos permite ordenar los riesgos según su importancia, calculada cuantitativa o cualitativamente.

c. La vulnerabilidad es el daño probable de una amenaza.

**7. Determine la opción que elegiría:**

a. Una salvaguarda que aporte mínimo retorno de la inversión.

b. Una contramedida que reduce un riesgo pero que tiene un precio alto.

c. Cuando es muy bajo, se puede asumir el riesgo sin hacer nada, y sin ser necesario informar a la Dirección.

**8. Indique si es o no necesario verificar:**

a. La temperatura máxima a la que pueden funcionar los ordenadores. Si

b. El nivel de tensión eléctrica que llega habitualmente al CPD. Si

c. El grosor de los paramentos del CPD y su construcción. Si

d. La existencia de pasos bajo el falso techo, entre el CPD y los recintos anexos. Si

**9. Indique una salvaguarda preventiva ante amenaza de inundaciones, y una reactiva.**

Salvaguarda preventiva: alarma

Salvaguarda reactiva: evacuación de agua

**10. Indique 5 salvaguardas ante el riesgo de incendios en el CPD.**

Sistema de caída de rayos

Conexiones correctas a los equipos

Condiciones de temperatura adecuadas

Sistema de cableado estructurado

Chequeos periódicos generales

**11. Indique 3 salvaguardas ante la difusión de software dañino.**

Copias de seguridad

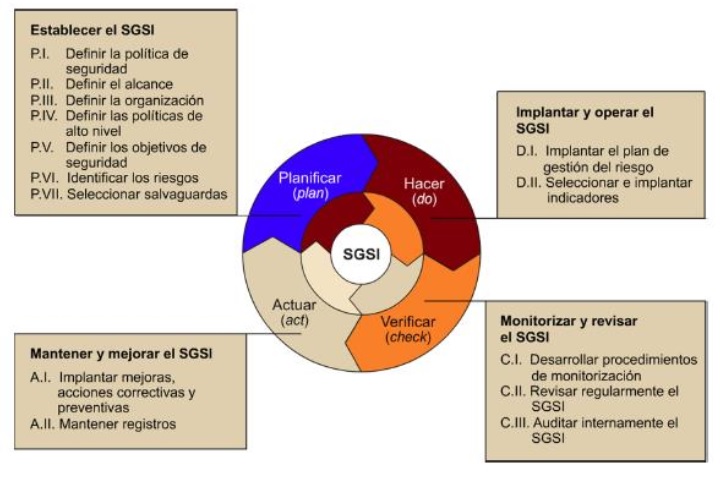
Procedimientos de reinstalación y configuración del sistema

Software de eliminación de virus y de eliminación de software malicioso

**12. ¿Qué contraseña será más compleja, una que tenga 5 dígitos, o una que tenga 3 caracteres usando mayúsculas o minúsculas?**

La segunda opción es más óptima; no obstante, la longitud mínima de la contraseña debe ser de 8 caracteres con mayúsculas y minúsculas, salvo en entornos de alta seguridad, donde se recomienda el mismo principio pero con 14 caracteres.

**13. Dibuje el diagrama de mejora continua de Deming.**



**14. ¿Cuáles de las siguientes salvaguardas no protegen a la información frente a la amenaza específica de los trabajadores?**

a. Cláusulas de responsabilidades legales en los contratos.

b. Un sistema de identificación y autenticación de usuarios.

c. Investigar los antecedentes.

**15. Un SGSI...**

a. ... permite implantar medidas de seguridad concretas para una amenaza.

b. ... corrige errores de implantación en las medidas de seguridad

c. ... puede considerar los datos de carácter ético y cultural de la empresa.