**JAVIER PRUNELL ACOSTA**

**MF0486\_3: Unidad de Aprendizaje 1 - Ejercicios de Repaso y Autoevaluación**

**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.\_\_\_\_\_\_\_\_\_\_\_\_\_\_ es que la información esté disponible siempre que se necesite.

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

c. \_\_\_\_\_\_\_\_\_\_\_\_\_es que la información sea válida, exacta, y completa.

d. \_\_\_\_\_\_\_\_\_\_\_\_\_o \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ y unas \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**6. Complete las siguientes definiciones:**

a. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ permite la elección de unas salvaguardas u otras, según unas directrices empresariales.

b. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ permite ordenar los riesgos según su importancia, calculada cuantitativa o cualitativamente.

c. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 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.

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

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

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

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

* Ante la amenaza de una inundación, una medida preventiva es no colocar el CPD cerca de tuberías o sistemas de riegos. Eliminar el sistema antiincendios por agua contemplado en algunos de los sistemas de prevención de incendios.
* La reactiva más adecuada será poner un falso suelo, con sistema de bombas para extraer el agua que pueda entrar. También debemos tener en cuenta el sistema TIER de certificación de servidores y Data Center (UNE 71504:2008)

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

* Evitar que en el lugar donde se haya instalado el CPD exista cualquier material combustible.
* Instalar sistemas de vaciado de oxigeno para consumirlo ante un posible incendio. En el pasado se utilizaba gas neón, pero era una solución perjudicial si existía alguien en el CPD. En muchas otras ocasiones, los sistemas CPD tienen un sistema de extracción de oxigeno de manera habitual ya que, sin este, un incendio es menos improbable.
* Instalar sistema de extintores no dañinos para los sistemas electrónicos: CO2 (ABC)
* Permisos para las personas con acceso restringido y prohibición de acceso con elementos inflamables o combustibles.
* Revisión semanalmente de los sistemas del cableado, contactos y sistemas electrónicos para evitar cortocircuitos.

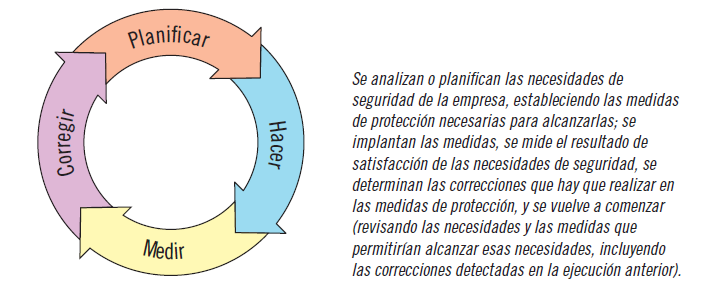
**11. Indique 3 salvaguardas ante la difusión de software dañino.**

* Actualización de los sistemas operativos para evitar que este software dañino utilice las vulnerabilidades del SO para poder realizar alguna acción maliciosa.
* Instalación de software antimalware y configuración de firewall. Bloqueo de los puertos más vulnerables y reforzar la contraseña de acceso al SO.
* A nivel de red, redirigir todas las conexiones entrantes a nuestra red a una zona desmilitarizada DMZ.

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

Cuando hablamos de contraseñas, debemos determinar que, en relación a los dígitos la complejidad es simplemente de 10 combinaciones en una de 5 dígitos, estaríamos hablando de 99999 de combinaciones. En cambio, en una contraseña de 3 caracteres cada uno, tendríamos una complejidad de 28 caracteres en mayúsculas y otras 28 en minúsculas. Por lo tanto, tendríamos un total 48 factorial (48!). Siempre una contraseña con caracteres tendría mas cantidad de combinaciones y por lo tanto, más compleja.

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



El diagrama de Deming, hace referencia al análisis o la planificación de las necesidades básicas de la empresa. Los resultados de la implementación de este ciclo permiten a las organizaciones una mejora integral de la competitividad, de los productos y servicios, mejorando continuamente la calidad, reduciendo los costos, optimizando la productividad, reduciendo los precios, incrementando la participación del mercado y aumentando la rentabilidad.

**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.