**RUNE BRITO NUÑEZ**

**SEGURIDAD INFORMATICA**

**MF0486\_3. UD6 – RESPUESTAS:**

1. **Complete el siguiente párrafo:**

La Seguridad física se ocupa de barreras físicas\_, procedimientos, y \_mecanismos\_ de control, para proteger los activos de las amenazas\_ físicas. La seguridad lógica se ocupa del conjunto de barreras lógicas, procedimientos, y mecanismos\_ de control para proteger los activos permitiendo el acceso lógico solo a los agentes autorizados.

1. **Enumere al menos 3 medidas que deben seguirse de acuerdo con la norma ISO27002 para trabajar en áreas seguras**.

1 Controlar mediante tarjetas y/o claves, para mantener el registro de auditorías de acceso

2 El deber de llevar identificación visible

3 revisiones periódicas, así como actualización de los derechos de acceso

1. **Indique cuál de las siguientes es la amenaza física más frecuente:**

1. El incendio.

2. La falta de suministro eléctrico.

3. El incidente causado por el infractor accidental, que actúa sin saber lo que se está haciendo o por error.

4. El secuestro o chantaje.

1. **De entre las siguientes afirmaciones, indique cuál es verdadera y cuál es falsa:**

a. Para la seguridad ambiental del CPD, deben ubicarse detectores de agua en el CPD, CCTV, vías de evacuación señalizadas, y carteles desaconsejando el consumo de bebidas y de comida.

 Verdadero

 Falso

b. Para la seguridad ambiental del CPD, deben aplicarse medidas contra fallos eléctricos, equipos de control de la temperatura y humedad, medidas contra incendios, detectores de agua, planes de evacuación, y la prohibición de entrar comida y bebida.

Verdadero

 Falso

c. Para la seguridad ambiental del CPD, deben aplicarse medidas que mantengan la temperatura en torno a los 21º ± 3º, y una humedad cercana al 50 %, que evite el riesgo de condensación y de electricidad estática.

Verdadero

 Falso

d. Para la seguridad ambiental del CPD se recomienda usar ventanas siempre que estén reforzadas mediante rejas y cristales opacos, que eviten ver la actividad que se desarrolla en su interior.

 Verdadero

Falso

1. **Empareje las siguientes contramedidas y amenazas:**

a. Interrupción breve del suministro. -

b. Caída de rayos. -

c. Interferencias o ruido eléctrico. -

d. Interrupción prolongada del suministro. -

1. **Enumere 6 medidas contra los incendios que recomendaría aplicar en un CPD.**

1 Paredes, techos y suelos a prueba de incendios, que cierren el recinto

2 Puerta con alto grado de protección frente al fuego

3 Detectores de humo

4 Alarmas de incendio manuales, en sitios estratégicos

5 Extintores manuales

6 Sistemas de extinción de incendio automático

1. **Empareje las siguientes tecnologías y su ámbito:**

a. Active Directory (directorio activo). \_\_

b Kerberos. \_\_

c. Login (nombre de usuario). \_\_

d. OpenLDAP. \_\_

1. **Complete la siguiente frase:**

Laslistasde control de **\_**acceso para un fichero o directorio, definen qué usuarios autenticados pueden acceder al fichero, y qué tareas pueden realizar. En sistemas Windows, se pueden modificar con el comando cacls y en sistemas Linux, con el comando ls-l

1. **Indique las cuatro características básicas que debe cumplir una contraseña de calidad.**

1 Contiene al menos, seis caracteres

2 No contiene “Administrador” o “Admin”

3 Combine mayúsculas, minúsculas y números

4 Que contenga caracteres no alfanuméricos

1. **Seleccione la mejor opción en relación a la política de escritorio limpio:**

a. Evita el riesgo de incendio, y es una medida de seguridad física.

b. Evita el acceso a información confidencial, especialmente fuera del horario normal de trabajo

c. Es un mecanismo de impresión segura.

d. Eliminando la acumulación se reduce la posibilidad de borrar un documento.

1. **Enumere 5 salvaguardas para reducir los riesgos de acceso al sistema operativo.**
2. Política sobre el uso de los servicios de red
3. Autenticación de usuario para los usuarios remotos, o conexiones externas
4. Identificación del equipo automática
5. Protección de puertos de diagnóstico y configuración remota
6. Segregación de redes
7. **Seleccione la opción correcta. Los métodos de autenticación se clasifican en...**

a. ... métodos débiles, fuertes y biométricos.

b. ... métodos con alta tasa de falsos positivos y métodos de alta tasa de falsos negativos.

c. ... métodos basados en algo que se sabe, métodos basados en algo que se tiene, y métodos basados en algo que es (o métodos biométricos).

d. ... métodos técnicos, organizativos, físicos y de personal.

1. **Enumere 3 métodos de autenticación para cada uno de los factores de autenticación.**

-Algo que se tiene; 1) llaves. 2) documento oficial. 3) smartcard

- Algo que se sabe; 1) contraseña. 2) código de acceso. 3) respuesta a una pregunta (desafío-respuesta)

- Algo que se es: 1) huella dactilar. 2) reconocimiento de voz. 3)patrón ocular de iris o retina

**14. Seleccione la opción más adecuada:**

a. No es necesario registrar la actividad del administrador, porque la empresa deposita en él la confianza del sistema de información.

b. Es especialmente importante registrar la actividad del administrador, porque actúa normalmente con privilegios.

c. Es especialmente importante registrar la actividad del administrador, porque estos puestos suelen tener mucha rotación.

d. No es necesario registrar la actividad del administrador, porque este tiene capacidad para desactivar el registro de auditoría.

1. **La norma ISO 27002 define un documento para recoger las directrices a partir de las que cuales se redacten los diferentes procedimientos, necesarios para llevar a cabo el control de acceso lógico. Se denomina...**

a. ... documento de seguridad.

b. ... normativa de control de acceso.

c. ... política de control de acceso

d. ... protocolo de control de acceso