**RUNE BRITO NUÑEZ**

**SEGURIDAD INFORMATICA**

**MF0486-3. UD8. Ejercicios de repaso y autoevaluación.**

**1.Elija la opción correcta:**

a. No hay que cambiar las contraseñas por defecto, basta desactivar los usuarios por defecto.

b. Deben cambiarse las contraseñas por defecto, y siempre que sea posible, deshabilitar los usuarios por defecto.

c. Siempre que sea posible, se debe cambiar el nombre de los usuarios por defecto.

**2. Empareje las opciones adecuadas:**

a. Superusuario.

b. Invitado.

c. Privilegios.

d. Acceso anónimo.

**3. Indique cuál de entre las siguientes afirmaciones no es una recomendación de la norma ISO 17799:2005 para las contraseñas:**

a. Que se evite la reutilización de claves anteriores.

b. Que se cambien regularmente.

c. Que sean fáciles de recordar.

d. Que tengan un periodo de validez mínimo.

**4. Indique cuál de las siguientes recomendaciones para la construcción de contraseñas se adapta a lo recomendado por CIS:**

a. Que sean cuanto más largas mejor, que sean complejas, que se cambien cada 90 días, y que no coincidan con las anteriores.

b. Que tengan sobre 8 caracteres, que se cambien regularmente (al menos cada 2 meses), pero no de manera diaria, y que no coincidan con las últimas 30   
 contraseñas**.**

c. Que tengan 8 caracteres, o 12 en entornos muy seguros, que tengan un periodo de vigencia de 1 día, que no coincidan con las últimas 24 contraseñas   
 empleadas.

d. No hay ninguna recomendación precisa, porque cuanto más larga sea la contraseña mejor.

**NOTA: VER PAG. 427 ->** ( La ongitud mínima de la contraseña de 8 caracteres, salvo en entornos de alta seguridad, donde se recomiendan 14 caracteres. Edad máxima de la contraseña de 60 días. Histórico de contraseñas a recordar, para no repetir ninguna de las últimas 24 contraseñas empleadas.) **Por ende, la más parecida es la opción “C”.**

**5. Complete la siguiente frase:**

En un ataque de fuerza bruta se prueban todas **las posibles contraseñas**, de 1 **carácter**, de 2, de 3, etc., mientras que en un **ataque**  de **diccionario** se prueban todas las palabras contenidas en listas de uno o varios idiomas.

**6. Enumere 3 recomendaciones respecto a la instalación de software de la guía CCN–STIC 821.**

1. Solo el personal de soporte técnico autorizado podrá instalar software en los equipos informáticos o de comunicaciones de los usuarios, con la excepción de las herramientas de uso común, que puedan ser descargables desde servidores internos.
2. Los usuarios podrán solicitar la inclusión de una aplicación, lo que debe ser estudiado, al menos por el personal técnico de seguridad.
3. No se podrá instalar software que no disponga de licencia correspondiente, o cuya utilización no sea conforme con la legislación vigente en materia de propiedad intelectual.

**7. Una pasarela también se llama...**

a. ... puente de comunicaciones.

b. ... Firewall.

c. ... puerta de enlace.

d. ... Router adaptado.

**8. Señale si las siguientes afirmaciones son verdaderas o falsas, desde la perspectiva de la seguridad de la información:**

a. Preferiblemente, una aplicación debe estar en varios servidores, por si alguno falla.

 Verdadero

Falso

b. Idealmente, las aplicaciones deben instalarse en pocos servidores, para reducir el número de equipos a proteger.

Verdadero

 Falso

c. Generalmente, una aplicación debería estar en un servidor dedicado a esta única función.

 Verdadero

 Falso

**9. Establezca las parejas:**

a. Criptosistemas de clave privada..

b. Criptosistemas de clave asimétrica.

c. Criptosistemas de clave simétrica  
 d. Criptosistemas de clave pública.

**10. Indique las alternativas seguras a los siguientes protocolos:**

a. HTTP.  **🡪 https**

b. Telnet. **🡪 SSH**

c. SMTP.  **🡪 ESMT**

**11. Indique si las siguientes afirmaciones son verdaderas o falsas:**

1. Los sistemas, especialmente los servidores, deben mantenerse permanentemente actualizados, siendo conveniente la aplicación automática de parches y correcciones.

 Verdadero

 Falso

1. La búsqueda activa de información y seguimiento de aparición de nuevas vulnerabilidades es una medida de protección para los sistemas.

 Verdadero

 Falso

1. Disponer de un inventario actualizado y completo de las aplicaciones que detalle al menos, el fabricante, las versiones, y los responsables de la aplicación, es una medida de protección para los sistemas.

 Verdadero

 Falso

**12. Indique el nombre de las siguientes aplicaciones maliciosas:**

- Aplicación que registra todas las pulsaciones de teclado. 🡪 **CAPTURADOR DE TECLADO** (Keylogger)

- Aplicación que envía información del equipo a un ordenador remoto. 🡪 **ESPIA** (Spyware)

- Aplicación que permite acceso al sistema operativo, aplicación o página web, eludiendo los controles de acceso que haya. 🡪 **PUERTA TRASERA** (Backdoor)

- Aplicación que no infecta a otros ficheros ejecutables, sino que constituye un fichero por sí mismo. 🡪 **GUSANO**

- Aplicación que permite al atacante tomar el control total del sistema como su administrador. 🡪 **HERRAMIENTAS DE CONTROL TOTAL** (Rootkit)

**13. Una medida principal de protección básica de las comunicaciones es:**

a. Emplear un firewall para separar internet de la red privada de la empresa.

b. Instalar un antivirus para protegerse de las amenazas constantes de código malicioso.

c. Separar en redes diferentes, por usuario, por servicio, o por sistema.

d. Que todo el tráfico esté cifrado usando IPsec.

**14. El protocolo que permite establecer las medidas de control para que un ordenador solo pueda conectarse a una toma concreta del switcher, y por lo tanto a una toma de red concreta del edificio, es el siguiente:**

a. El protocolo de LACP (Link Aggregation Control Protocol, IEEE 802.1ax).

b. Protocolo de transporte SSL/TLS.

c. IEEE 802.1X.

d. IPsec.

**15. Complete la siguiente frase:**

Los registros se deben proteger para que un atacante no los modifique o elimine, para lo cual una de las posibles soluciones es **guardar** los **registros** en un **servidor diferente** dedicado a ello.