**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.

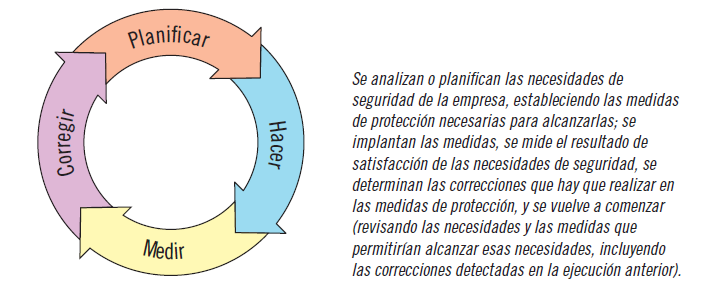
**11. Indique 3 salvaguardas ante la difusión de software dañino.**

* 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.

**MF0486\_3 : Unidad de Aprendizaje 2 - Ejercicios de Repaso y Autoevaluación**

**1. Complete la siguiente oración:**

En el BIA se estudian cuáles son los procesos o **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** del negocio, que dependan en cualquier medida de los sistemas de información.

**2. Indique qué 3 resultados básicos entrega el BIA:**

**3. Indique si las siguientes afirmaciones son verdaderas o son falsas.**

a. Para realizar un BIA, basta pasar unos formularios a los responsables de departamento, para que evalúen la importancia de su función última, y determinen cuánta información podrían perder.

 Verdadero

Falso

b. El BIA es una herramienta para estudiar la continuidad del negocio.

Verdadero

 Falso

c. El BIA asegura que el RTO será el que indiquen los dueños de los procesos de negocio críticos.

Verdadero

 Falso

**4. Marque la respuesta correcta:**

a. El RTO siempre será mayor que el RPO, porque no se puede adivinar la información futura de la empresa.

b. El RTO representa el periodo de tiempo del que se pierde información.

c. El tiempo total que pierde la empresa es la suma del RPO y el RTO

**5. Determine la opción que elegiría, en base a una criterio de máxima integridad:**

a. Una salvaguarda que asegura que la información sea exacta y completa.

b. Una contramedida que proporciona una RTO alta a un precio bajo.

c. Un método de recuperación de precio alto, que proporciona un RTO muy bajo, y un RPO moderado.

**6. Enumere cuatro aspectos que pueden considerarse a la hora de evaluar el daño que un incidente de seguridad causa en una función de la empresa:**

**7. Determine la fórmula más aproximada:**

a. Proceso = seguridad + personas + sistemas.

b. Proceso = información + personas + equipos

c. Proceso = seguridad + información + personas.

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

a. El dueño de la empresa debe poder acceder a toda la información.

b. El acceso a la información solo debe proporcionarse a quien desempeñe el rol de consultor en los procesos críticos de negocio.

c. Los permisos de acceso a la información siempre debe ser los mínimos necesarios.

**9. Complete las siguientes definiciones:**

a. La información **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**difundida sin control, puede suponer incumplimientos legales.

b. La información **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** siempre requiere de esta calificación, expresa por el área o responsable de comunicación de la empresa.

c. La información **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** puede ser accedida libremente por todo el personal de la empresa, incluso los no empleados.

**10. Califique las dimensiones de seguridad, según nivel alto, medio, o bajo:**

a. De disponibilidad, si se precisa siempre.

b. De confidencialidad, como un listado de teléfonos de la empresa.

c. De integridad, en una base de datos en la que se admite hasta un 10 % de registros erróneos sin ningún impacto.

d. De confidencialidad, como la información que se ha publicado en la web.

**11. Si los requisitos CIA de dos componentes de un proceso son (4, 4, 5) y (3, 2, 6), determine los requisitos CIA del proceso total, en los siguientes casos:**

a. Si se agregan.

b. Si se emplea el más alto.

c. Si los procesos se agregan, las tareas del proceso implican que su integridad sea el doble de importante, y se busca un único valor de la seguridad.

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

a. Los requisitos de confidencialidad para una persona dependen de cómo sea de reservado.

 Verdadero

Falso

b. Los requisitos de integridad de una persona dependerán de si acepta o no sobornos.

 Verdadero

 Falso

c. Los requisitos de disponibilidad de una persona dependerán de que siempre tenga un móvil encendido.

 Verdadero

 Falso

**13. Indique 3 servicios de soporte básico que puedan ser componentes de un proceso en el que intervengan sistemas de información:**

Suministro eléctrico, la climatización, o el alojamiento de los equipos.

**14. Elija una contramedida para subsanar el riesgo de integridad de las copias de seguridad de la información:**

a. Almacenarlas comprimidas.

b. Guardar las copias protegidas por contraseña o cifradas.

c. Guardar el hash de la información para verificar la copia antes de restaurarla

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

(1)

Coste

Tiempo

(2)

**MF0486\_3 : Unidad de Aprendizaje 3 - Ejercicios de Repaso y Autoevaluación**

**1. Complete la siguiente oración:**

Por simplicidad, el análisis y gestión de riesgos se suele acortar a **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, 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:**

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

**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 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ o **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** , 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.**

**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.

b. El riesgo acumulado.

c. El impacto acumulado.

d. El riesgo repercutido.

**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

**MF0486\_3 : Unidad de Aprendizaje 4 - Ejercicios de Repaso y Autoevaluación**

**1. Empareje los siguientes términos, correspondientes a diferentes aspectos de cada fase de un SGSI:**

a. Establecimiento.

b. Monitorear y revisar.

c. Corregir.

d. Implementación y operación.

e. ¿Cómo modificar el rumbo?

f. Implantación de salvaguardas.

g. Planear.

h. ¿Dónde estamos?

**2. Si el nivel de seguridad CIA de un proceso es (4,5,1), y el nivel requerido es (1,8,1), el informe de insuficiencias concluirá que...**

a. ... el nivel de seguridad existente (4+5+1=10) cumple los requerimientos de seguridad de la empresa (1+8+1=10).

b. ... hay un déficit de 3 puntos en la integridad existente (5) frente a la requerida (8). Por tanto, integridad no alcanzada, inferior a 8: 5.

c. ... debe invertirse en mejorar la integridad.

d. No se indicará nada, porque no se alcanzan los valores de riesgo máximo admisibles.

**3. Una fuente para los requisitos de seguridad de una empresa es:**

a. El resultado de una auditoría de seguridad del cumplimiento de la norma ISO 27001.

b. El presupuesto de seguridad.

c. Los principios, los objetivos, y los requerimientos comerciales que el sistema de información debe cumplir para sostener las operaciones de la empresa.

d. Un método de valoración CIA de un proceso, coincidente con la valoración CIA de su información crucial.

**4. Elija la secuencia temporal de intervención de los controles:**

a. Organizativos, prevención, de detección física, emergencia, y recuperación.

b. Primero los de detección, luego los de emergencia, luego los de recuperación, y por último, los de prevención, para evitar que se repitan.

c. Preventivos, correctivos, y adaptativos o perfectivos.

d. Preventivos, de detección, de emergencia, y de recuperación.

**5. Bajo unos criterios generales, elija que conjunto de salvaguardas resulta óptimo:**

a. Medidas físicas y técnicas, para la detección y recuperación, pero muy difíciles de operar.

b. Medidas preventivas, de detección y recuperación, organizativas y técnicas, de complejidad moderada, y con un programa de actualizaciones periódicas.

c. Una aplicación de detección y recuperación integrada, que se ejecuta sola, y apenas necesita intervención humana cuando se activa, pero sin actualizar ni revisar desde hace años.

d. Las más económicas que cumplan la legislación vigente.

**6. ¿A qué tipo de activo aplican las siguientes salvaguardas, según el método MAGERIT?**

**7. Según ISO 17779, e ISO 27002, los controles esenciales son los siguientes:**

a. La protección de datos y privacidad de la información, los derechos de propiedad intelectual, y la protección de los registros de la empresa.

b. El marco regulatorio, los objetivos organizacionales, los requerimientos y restricciones de operación, un costo de implementación en relación al riesgo que se reduce proporcional a los requisitos de la empresa, y el equilibrio entre coste de implementación y el riesgo.

c. 133 controles, agrupados en 39 objetivos de 11 dominios básicos.

d. No existen unos controles esenciales, porque dependen del sector de actividad de cada empresa.

**8. Indique qué controles deben incluirse en una declaración de aplicabilidad:**

Controles seleccionados, Controles existentes y Controles excluidos.

**9. Complete la siguiente frase:**

El Esquema Nacional de Seguridad establece la política de seguridad en la utilización de medios electrónicos, y está constituido por **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** y **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** para una adecuada SI.

**10. Indique a qué fase de un SGSI pertenecen las siguientes tareas:**

- Identificar los riesgos

- Tomar medidas preventivas y correctivas.

- Revisar evaluaciones de riesgo.

- Definir efectividad controles.

- Analizar y evaluar los riesgos.

- Plan de tratamiento de riesgos.

- Detección y respuesta a incidentes.

- Seleccionar controles para riesgos.

**11. Según ISO 27001, el plan de tratamiento de riesgos, debe identificar:**

**12. Los procesos de la norma ISO 27003, que dan pautas sobre la información que se debe recoger de cada control o salvaguarda, lo que resulta muy valioso para su implantación, son:**

a. La revisión del marco legislativo, las normas y requisitos operacionales, los principios, y objetivos (incluidos los comerciales) que debe cumplir el   
 sistema de información para sostener las operaciones de la empresa.

b. El análisis y gestión de riesgos, la elaboración de una declaración de aplicabilidad, y una auditoría que concluya en un informe de insuficiencias.

c. El diseño de contramedidas en la seguridad organizacional, y el diseño de contramedidas en seguridad física y de las TIC.

d. Los mismos que se marcan en la norma 17799:2005.

**13. Enumere el contenido recomendado para cada acción a ejecutar dentro del plan de tratamiento de riesgo, según las normas ISO 27000:**

**14. Enumere el contenido recomendado de cada programa de seguridad, según MAGERIT:**

**15. A la vista de las siguientes curvas de comparación de pérdidas y ganancias, elija la mejor opción:**

**MF0486\_3 : Unidad de Aprendizaje 6 - Ejercicios de Repaso y Autoevaluación**

1. **Complete el siguiente párrafo:**

La Seguridad física se ocupa de barreras **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,** procedimientos, y **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** de control, para proteger los activos de las **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**físicas. La seguridad lógica se ocupa del conjunto de barreras **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, procedimientos, y\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de control para proteger los activos permitiendo el **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**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**.
2. **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.**
2. **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:**

Las **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**de control de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** 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**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, y en sistemas Linux, con el comando **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**.

1. **Indique las cuatro características básicas que debe cumplir una contraseña de calidad.**
2. **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. **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.**

**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

**MF0486\_3 : Unidad de Aprendizaje 7 - Ejercicios de Repaso y Autoevaluación**

**1. Complete la siguiente oración:**

La arquitectura de red más extensamente utilizada, es la arquitectura **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**. Esta arquitectura define las comunicaciones, organizándolas en diferentes niveles o capas.

**2. Enumere las capas en que se organizan los protocolos de la arquitectura de red de internet:**

**3. Determine la opción válida:**

a. Los protocolos TCP e IP son protocolos de la capa de red.

b. El protocolo HTTP, FTP, y SMTP, son protocolos de la capa de aplicación.

c. Ethernet es un protocolo de la capa de nivel físico.

d. Todas las respuestas anteriores son incorrectas.

**4. Empareje los siguientes conceptos:**

a. Dirección MAC.

b. Dirección IP.

c. Número de puerto.

**5. Determine el nombre de cada segmento de puertos:**

a. 0...1023.

b. 1024...49151.

c. 49152...65535.

**6. Indique los puertos para los siguientes 4 servicios básicos:**

a. Navegación web

b. Transferencia de ficheros

c. Navegación web segura

d. Envío de correo electrónico

**7. Complete la siguiente frase:**

Orientado a conocer todas las conexiones activas del nodo donde se ejecuta, **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** permite saber en un momento dado qué puertos TCP y UDP se están usando, además de estadísticas de uso.

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

a. Para probar si hay conexión con un equipo, emplearía la herramienta traceroute.

b. Empleando whois puede conocer la dirección o domicilio donde está físicamente alojado un servidor.

c. Para conocer la ruta de conexión, emplearía la ruta traceroute.

d. Empleando ping puede saberse si hay conexión en un puerto TCP concreto.

**9. Seleccione la aplicación adecuada:**

a. Para realizar múltiples intentos de conexión.

b. Para establecer una conexión en un puerto.

c. Para interpretar la mayoría de protocolos y devolver, información adicional a los puertos abiertos.

**10. Complete la siguiente frase:**

La realización de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** sobre una máquina ajena puede considerarse una actividad peligrosa, incluso ser constitutiva de delito.

**11. El inconveniente de las herramientas que registran las conexiones en 1 instante de tiempo es que...**

a. ... no tienen ningún inconveniente, y de hecho, nmap es un estándar de facto.

b. ... no pueden devolver la dirección del destino, porque no esperan el ACK.

c. ... la salida siempre es por pantalla, aunque la ejecución puede ser continua.

d. ... no capturan las conexiones que se produzcan entre diferentes ejecuciones.

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

a. La herramienta Microsoft Port Reporter aumenta las garantías de registrar una conexión de red.

Verdadero

 Falso

b. Las herramientas de registro continuo tienen la ventaja añadida de precisar poco espacio para almacenar los logs, porque los sobrescriben.

 Verdadero

 Falso

c. Siempre es preferible usar una herramienta de registro continuo, en lugar de una herramienta de registro puntual.

 Verdadero

 Falso

**13. Indique la opción más adecuada:**

a. Para conocer el tráfico de un servidor, hay que instalarle un sniffer.

b. Para conocer el tráfico de un servidor, se puede instalar un sniffer a un pc con el que comparta cualquier switcher.

c. Para conocer el tráfico de un servidor, se puede instalar un sniffer a un pc con el que comparta un hub.

d. Para conocer el tráfico de un servidor, se deben consultar sus registros de auditoría.

**14. En relación a las herramientas TCPDUMP y TCPFLOW, indique si las afirmaciones son verdaderas o falsas:**

a. Se pueden usar como entrada para WireShark.

 Verdadero

 Falso

b. Son muy eficientes para capturar tráfico desde línea de comandos.

Verdadero

 Falso

c. Pertenecen a la categoría de sniffers.

Verdadero

Falso

**15.Complete la siguiente frase:**

La herramienta **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**permite construir **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** que eliminen todo el tráfico que no interesa, por ejemplo, porque corresponda a servicios conocidos que no se quieran analizar.

**MF0486\_3 : Unidad de Aprendizaje 8 - 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 los 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.

**5. Complete la siguiente frase:**

En un ataque de fuerza bruta se prueban todas las\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de 1 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, de 2, de 3, etc., mientras que en un **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** 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.
4. Se prohíbe la reproducción, modificación, transformación, cesión, comunicación, o uso fuera de la empresa de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la empresa.
5. No se podrán deshabilitar o eliminar las aplicaciones instaladas por la empresa, especialmente las relacionadas con la seguridad.

**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.

b. Telnet.

c. SMTP.

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

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

 Verdadero

 Falso

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

 Verdadero

 Falso

c. 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.

- Aplicación que envía información del equipo a un ordenador remoto.

- Aplicación que permite acceso al sistema operativo, aplicación o página web, eludiendo los controles de acceso que haya.

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

- Aplicación que permite al atacante tomar el control total del sistema como su administrador.

**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 **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**los **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** en un **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**dedicado a ello.

**MF0486\_3 : Unidad de Aprendizaje 9 - Ejercicios de Repaso y Autoevaluación**

**1. Indique cual de las siguientes recomendaciones del Esquema Nacional de Seguridad es la correcta:**

a. Se debe emplear un sistema de seguridad perimetral que prohíba todo el tráfico.

b. Se debe emplear un sistema cortafuegos que separe la red interna del exterior, y que permita pasar los flujos autorizados.

c. Se debe emplear un firewall que separe la red interna del exterior, por el que pase todo el tráfico, y que solo deje progresar el autorizado previamente.

d. Solo se recomienda emplear firewalls en entornos de seguridad de nivel alto.

**2. Enumere 3 técnicas de ingeniería social que podría emplear un atacante para obtener información del sistema objetivo.**

**3. Señale cuáles de las siguientes afirmaciones son verdaderas y cuáles son falsas:**

a. Los ataques que pueden sufrir las comunicaciones de emisor a receptor son amenazas físicas o de interrupción y amenazas lógicas.

 Verdadero

 Falso

b. Las comunicaciones sufren un ataque de fabricación, cuando se consigue e introduce en el flujo de comunicaciones un mensaje similar al atacado.

 Verdadero

 Falso

c. Las comunicaciones solo pueden sufrir ataques de interrupción (disponibilidad), interceptación (confidencialidad) y fabricación (integridad).

 Verdadero

 Falso

**4. Indique el nombre de los siguientes tipos de cortafuegos.**

- Equipo que solo puede realizar filtrado de paquetes.

- Equipo que crea un canal de comunicación entre cliente y servidor para todo tipo de aplicación del cliente.

- Equipo que recuerda las comunicaciones iniciadas desde la LAN a internet para admitir automáticamente los paquetes de respuesta de internet a la LAN.

**5. Empareje los opciones adecuadas:**

1. Screened subnet.

2. Bastión de una red.

3. Bastión filtrado.

4. Screened host.

5. Router de filtrado.

6. Subred filtrada.

7. Screening router.  
 8. Single homed host.

**6. Complete la siguiente frase:**

La función NAT permite **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** una dirección **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** entre todas las **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** privadas de los clientes LAN.

**7. Enumere al menos 3 ventajas de un cortafuegos construido mediante un bastión, frente a un firewall construido mediante un router.**

**8. Complete la siguiente frase:**

En un firewall screened host se emplea un **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** previo al bastión para **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**los **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, y que está configurado para que solo envíe hacia el bastión el **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** filtrado, y para que solo admita conexiones internas desde el **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**9. Señale si las siguientes afirmaciones son verdaderas o son falsas:**

a. Un firewall screened subnet consta de 3 elementos.

 Verdadero

 Falso

b. Un firewall de subred filtrada es el diseño más seguro, porque aún comprometido el bastión, el atacante debe sobrepasar otro router de filtrado.

Verdadero

 Falso

c. Un firewall de subred filtrada es el único diseño que define una zona DMZ para proteger servidores que deban ser accedidos desde el exterior.

 Verdadero

 Falso

**10. Establezca las parejas**

a. Redes señuelo.

b. Rangos de direcciones de red diferentes.

c. Honeypot.

d. Segregación en subredes.

e. Ubicación de servidores accesibles desde el exterior.

f. DMZ

**11. Indique si se deben prohibir o permitir los siguientes flujos de red en un diseño screened subnet, que incorpora un servidor bastionado en la zona DMZ accesible desde internet, que necesita acceder a un servidor de base de datos privado:**

a. Del servidor bastionado a la LAN.

b. Del servidor bastionado a internet.

c. Del servidor bastionado al servidor de base de datos.

d. De los clientes al servidor bastionado.

**12. Complete la siguiente frase:**

Las redes privadas virtuales permiten **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** o canales de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** empleando **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** no seguras o **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, como **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, usando para ello métodos **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, que permiten defender las comunicaciones de ataques de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** y de **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**.

**13. ¿Cómo se clasifican los tipos de VPN, de acuerdo a su uso?**

**14. Enumere 3 protocolos empleados para construir redes privadas virtuales, indicando la capa de red en la que actúan, y sus variantes o modos de funcionamiento si los hay.**

**15. Indique dos contramedidas adicionales al empleo de cortafuegos que deben aplicarse, para asegurar su eficacia y evitar una falsa sensación de seguridad:**