|  |  |  |  |
| --- | --- | --- | --- |
| **Nombre y Apellidos:** | **RUNE BRITO NÚÑEZ** | **Firma del Alumno:** |  |
| **DNI:** | 78852907-Y | **Firma del Profesor:** |  |

|  |  |  |
| --- | --- | --- |
| **Apto:** | **No Apto:** | **Calificación:** |

**Instrucciones Generales**

La puntuación máxima será de 10 puntos.

Esta prueba tendrá una duración máxima de 540 minutos

( Temporalizados durante la Unidad de Aprendizaje 1)

El alumno/a deberá acatar las siguientes normas durante la duración de la actividad:

* Rellene el encabezado con su nombre, apellidos y D.N.I.
* Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
* Usar exclusivamente bolígrafo azul o negro
* Guardar los ficheros generados en una carpeta con nombre **E1\_486\_3**
* El docente le indicará al final como entregar el contenido de dicha carpeta
* Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

**Equipo y material**

* Bolígrafo azul.
* Folios.
* Ordenadores.
* Conexión a Internet. ( Para buscar información a modo de ayuda )

**Instrucciones específicas**

**Nombre:** Realizar actividad teórica E1

**Agrupamiento:** Individual

**Descripción:** Los alumnos realizarán una serie de actividades teóricas pertenecientes al primer módulo formativo ( MF0486\_3 )

Recursos: [Libro de la Editorial IC MF0486\_3 – Seguridad en equipos informáticos](https://www.iceditorial.com/seguridad-informatica-ifct0109/6423-seguridad-en-equipos-informaticos-9788416271115.html)

**Duración:** 60 minutos

**Condiciones de realización:**

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumno podrá hacer uso de internet para su realización.

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

**OBSERVACIONES**

**CAPITULO – 01 //**

**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

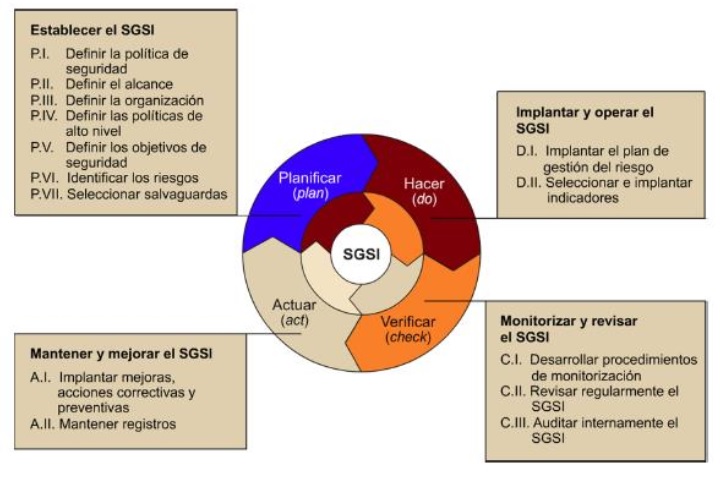
Procedimientos de reinstalación y configuración del sistema

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.

**CAPITULO – 02 //**

**MF0486\_3. UD2 – RESPUESTAS:**

**1. Complete la siguiente oración:**

En el BIA se estudian cuáles son los procesos o funciones vitalesdel negocio, que dependan en cualquier medida de los sistemas de información.

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

Del BIA se obtienen resultados de muchísimo valor:

1. Conocer cuáles son los activos informáticos que intervienen en los procesos críticos del negocio.

2. Ser capaces de evaluar su impacto.

3. Conocer cuáles son los requisitos de seguridad para estos activos (tiempo objetivo de restablecimiento, qué salvaguardas planificadas que se deben aplicar, etc.)

**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 un 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:**

El daño que genera en la función principal

El daño financiero de la función

El daño a otras funciones dependientes de esta

El daño en la imagen o reputación

El daño que genera en el nivel de satisfacción

**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 confidencial difundida sin control, puede suponer incumplimientos legales.

b. La información Confidencialsiempre requiere de esta calificación, expresa por el área o responsable de

comunicación de la empresa.

c. La información Público 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. alto

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

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

impacto. bajo

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

**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. (7,6,11)

b. Si se emplea el más alto. (4,4,6)

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. (M,M,A)

**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)

1. Coste de lasmedidas de recuperación
2. Coste de la parada

**CAPITULO – 03 //**

**MF0486\_3. UD3 – RESPUESTAS**

**1. Complete la siguiente oración:**

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

Conviene realizarlo cuando; la empresa dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión

Conviene realizarlo antes de emprender cambios profundos o realizar inversiones de renovación tecnológica

Será obligatorio para conducir una auditoría de seguridad, o definir el marco de cumplimiento de una ley

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

1. Requisitos legales
2. Requisitos operacionales
3. Objetivos de la empresa
4. Rentabilidad de la acción

**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 información o datos, 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.**

Capa 4: las funciones y procesos de la organización (objetivos, bienes,

y servicios producidos).

Capa 3: la información y los datos.

Capa 2: el sistema de información propiamente dicho (aplicaciones,

equipos, soportes, equipamiento auxiliar, y redes de comunicaciones).

Capa 1: el entorno que se precisa (equipamiento y suministros eléctricos

de climatización y de comunicaciones, el personal, y otros,

como el edificio o el mobiliario).

**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. Suma de las degradaciones de los activos pendientes

b. El riesgo acumulado. Riesgo por impacto acumulado de un activo a raíz de la frecuencia de su amenaza

c. El impacto acumulado. Impacto sobre el valor acumulado de un activo , a raíz de su amenaza

d. El riesgo repercutido. Riesgo total sobre el servicio

**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

1. **RESP: Coste de riesgo residual**
2. **RESP: Coste de salvaguardas**

**CAPITULO – 04 //**

**MF0486\_3. UD4 – RESPUESTAS:**

**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?**

\*Registro de intrusiones. 🡪 (Equipos)

\*Control de acceso de las entradas/salidas de personas y equipos. 🡪 (Seguridad Física)

\*Protección frente a dañino (virus, troyanos, etc.). 🡪 Aplicaciones

**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 el código 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 principios básicos y requisitos mínimos

para una adecuada SI.

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

~**~** Identificar los riesgos. (Establecer SGSI)

~**~** Tomar medidas preventivas y correctivas. (Mantener y mejorar SGSI)

~**~** Revisar evaluaciones de riesgo. (Monitorear y revisar SGSI)

~**~** Definir efectividad controles. (Implementar y operar SGSI)

~**~** Analizar y evaluar los riesgos. (Establecer SGSI)

~**~** Plan de tratamiento de riesgos. Implementar y operar SGSI

~**~** Detección y respuesta a incidentes. (Implementar y operar SGSI)

~**~** Seleccionar controles para riesgos. (Establecer SGSI)

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

Que identifique: La acción, los recursos , las responsabilidades, Las prioridades de la gerencia para manejar los riesgos y el ´SI`

**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:**

–– Descripción de la acción

–– Prioridad de riesgos de SI para gerencia, que apoya ejecutar la acción

–– Recursos necesarios para la acción

–– Consideraciones de financiación

–– Funciones y responsables en la ejecución de la acción

–– Medidas de eficacia de controles

–– Para cada control, aspectos del diseño de los controles para su

implantación:

–– Descripción detallada del control

–– Nombre de la persona responsable del diseño y la implantación

–– Prioridad de la implantación

–– Periodo de tiempo en que el control debe estar implantado

–– Tareas o actividades para implementar el control, detallados paso a paso

–– Recursos concretos para la implantación de este control

–– Persona a quien se debe informar que el control se ha implantado

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

• objetivo genérico

• prioridad o urgencia

• ubicación temporal: ¿cuándo se llevará a cabo?

• salvaguardas involucradas

• unidad responsable de su ejecución

• estimación de costes financieros

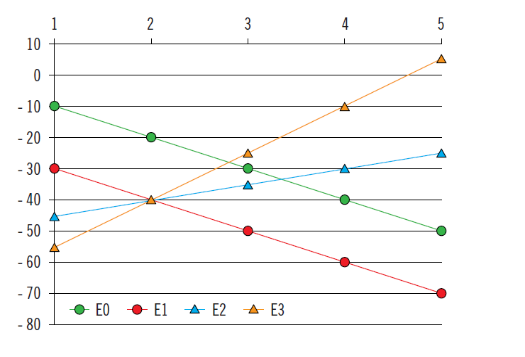
• estimación de recursos

• estimación de impacto para la organización

Fuente:>> [Libro II – Magerit - página 74](https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html)

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

**mejor opción:**



El caso más óptimo es el E3. Ya que es el de mayor inversión inicial, se obtiene rentabilidad en

el año 3, e incluso se obtienen beneficios operativos en el año 5.

**CAPITULO – 05 //**

**MF0486\_3. UD5 – RESPUESTAS:**

**1. Elija la opción correcta:**

1. La LOPD limita el uso de la informática, para garantizar el honor y la

intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

1. La Directiva 94/46/CE3, en materia de protección de datos, garantiza la libre circulación de datos entre los estados miembros.

c. La Constitución Española establece que la ley limitará el uso de la informática, para garantizar el

honor y la intimidad personal y familiar de los

ciudadanos, y el pleno ejercicio de sus derechos.

1. La protección de datos de carácter privado no está regulada en manera

alguna, y solo es una recomendación de la norma ISO 27000.

**2.Empareje los opciones adecuadas:**

1. Responsable del tratamiento.

2. Encargado del tratamiento.

3.Persona física o jurídica que trata los datos personales.

4. Persona física o jurídica, que decida sobre la finalidad, contenido, y uso

del tratamiento.

**3. Indique cuáles de entre los siguientes no son fuentes accesibles al público:**

a. Una guía telefónica de edición anual, y difusión a todos los clientes de una empresa de telefonía. (Según el artículo 28.3 no puede ser accesible)

b. Los diarios y boletines oficiales.

c. Un listado de una asociación de médicos, que incluye nombre, especialidad, y el domicilio.

d. Registro Mercantil.

**4. Indique, respondiendo sí o no, si las siguientes afirmaciones son objeto de la LOPD:**

1. Los datos de ciudadanos españoles de una empresa establecida fuera de la U.E. NO
2. Los datos de Fuerzas y Cuerpos de Seguridad referentes a investigaciones sobre organizaciones terroristas internacionales que puedan operan en España. NO
3. Un listado con los datos de contacto particular de sus conocidos, aficionados a las apuestas deportivas de futbol, que incluye sus números de cuenta para transferirles los beneficios. SI

**5. Marque la opción correcta**:

1. Los derechos ARCO son los derechos de acceso, revocación, cancelación, y ofuscación o cifrado.
2. Los DCP tienen los derechos ARCO, que aseguran su acceso, rectificación, cancelación, y oposición.
3. Los derechos ARCO son ejecutados por la Agencia Española de Protección de Datos, para proteger a los titulares de los datos.
4. Los derechos ARCO garantizan un poder de control sobre los datos, asegurando el derecho de acceso, el de rectificación, el de cancelación, y el de oposición.

**6. Enumere la/s condición/es necesarias para que, con su consentimiento expreso, puedan comunicar sus DCP:**

■ A los DCP que se usen para la prevención o diagnóstico médico, prestación de asistencia sanitaria, tratamiento médico, o gestión de servicios sanitarios; pero siempre por un profesional sanitario sujeto al secreto profesional, u otra persona sujeta a obligación equivalente de secreto. También podrán tratarse para salvaguardar el interés vital del afectado o de otra persona, en el supuesto que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

■ A los DCP que se usen para realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros, o cuando los DCP aparezcan de forma accesoria o incidental en ficheros no automatizados, y sin guardar relación con la finalidad del mismo (artículo 81-5).

■ A los DCP que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad, o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos (RLOPD artículo 81-6).

**7. Enumere la/s condición/es necesarias para que, sin su consentimiento expreso, puedan comunicar sus DCP:**

■Los que se refieran a ideología, afiliación sindical, religión, creencias, origen racial, salud, o vida sexual.

■ Los que se refieran a datos recabados para fines policiales, sin consentimiento de los afectados.

■ Aquellos derivados de actos de violencia de género.

■ A los datos de tráfico y de localización de los operadores que presten servicios de comunicaciones electrónicas, o exploten redes públicas de comunicaciones electrónicas, se les aplicarán además de las medidas de nivel básico y medio, la medida de nivel alto del artículo 103

**8. Califique las siguientes infracciones**

a. Divulgar DCP no respetando el deber de secreto. Grave

b. Obstaculizar el ejercicio de los derechos ARCO. Grave

c. No cumplir las medidas de seguridad del nivel reglamentario. Leve

d. No cumplir el deber de información al recabar DCP de sus titulares, y no haber solicitado su inscripción en la AEPD. Muy grave

**9. Indique la sanción esperable si se comunica a terceros un fichero sin estar legitimado para ello, reconociendo de manera espontánea la infracción:**

a. De 40.001 a 300.000, porque se trata de una infracción grave.

b. De 900 a 40.000, porque el reconocimiento espontáneo reduce la franja de sanciones a las de la categoría leve.

c. De 900 a 40.000, porque con el reconocimiento espontáneo la infracción pasa a ser de categoría leve.

d. Siempre que se reconozca la infracción, no habrá sanción alguna, por reducción.

**10. ¿Qué nivel de seguridad le aplicaría a los datos relativos a la afiliación sindical y salud, contenidos en el fichero de personal de su empresa?**

a. Básico.

b. Medio.

c. Alto.

d. Leve.

**11. Que exista un registro de incidencias donde se anoten las recuperaciones de DCP a raíz de un incidente, es una medida que se debe implantar desde el nivel (incluido)...**

a. ... básico.

b. ... medio.

c. ... alto.

d. No es una medida

**12. Realizar una copia de** **respaldo semanal de los DCP es una medida de nivel...**

a. ... básico.

b. ... medio.

c. ... alto.

d. No es una medida.

**13. Complete la siguiente frase:**

Deberá designarse uno o varios responsables de seguridad, para uno o todos los ficheros, encargados de coordinar y controlar las medidas de seguridad que se establezcan.

**14. Elija la respuesta más adecuada sobre el procedimiento a seguir para realizar la inscripción de un fichero de DCP:**

1. Se solicita la inscripción, se mandan los datos de los ficheros al Registro General de Protección de Datos, y por último, se espera hasta que la AEPD responda.
2. Siempre se debe notificar la solicitud de inscripción antes de la creación del fichero, y si no hubiera respuesta de la AEPD en 30 días, se sobreentiende que el fichero está inscrito.
3. No es necesaria ninguna inscripción, porque constituye una infracción LEVE, que se podría reconocer espontáneamente, para que no se aplicara ninguna sanción económica; por lo que bastaría inscribirlos después.
4. Se rellena el formulario de la agencia en internet, abonándose las tasas de inscripción según el nivel de las medidas que se quieran aplicar.

**CAPITULO – 06 //**

**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

1. **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

**CAPITULO – 07 //**

**MF0486\_3. UD7 – RESPUESTAS:**

**1. Complete la siguiente oración:**

La arquitectura de red más extensamente utilizada, es la arquitectura TPC / IP 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:**

* Capa física
* Capa de enlace
* Capa de red
* Capa de transporte
* Capa de sesión
* Capa de presentación
* Capa de aplicación

**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.

1. **Empareje los siguientes conceptos:**

a. Dirección MAC. – Capa de transporte

b. Dirección IP. – Capa de acceso o enlace

c. Número de puerto. – Capa de inter-red

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

a. 0...1023. Puertos del sistema o bien conocidos

b. 1024...49151. Puertos registrados o de usuario

c. 49152...65535. Puertos dinámicos o privados

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

a. Navegación web El puerto 80

b. Transferencia de ficheros El puerto 22

c. Navegación web segura El puerto 443

d. Envío de correo electrónico El puerto 25

**7. Complete la siguiente frase:**

Orientado a conocer todas las conexiones activas del nodo donde se ejecuta**,** netstatpermite 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. Superscan

b. Para establecer una conexión en un puerto. Portquery

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

Nmap

**10. Complete la siguiente frase:**

La realización de sondeos exhaustivossobre 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 **\_**wireshark permite construir filtros que eliminen todo el tráfico que no interesa, por ejemplo, porque corresponda a servicios conocidos que no se quieran analizar.

**CAPITULO – 08 //**

**MF0486\_3. UD8 – RESPUESTAS:**

**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 longitud 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.

**CAPITULO – 09 //**

**MF0486\_3. UD9 – RESPUESTAS:**

**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.**

1. **Ataque de interrupción**, consistente en que un objeto del sistema no esté disponible.

2. **Ataque de interceptación**, consistente en que una persona o programa consiga tener un acceso no autorizado a un objeto del sistema.

3. **Ataque de modificación,** consistente en que, además de lograr interceptar un objeto, se logre modificarlo; lo que puede incluir la destrucción completa y por tanto la interrupción.

4. **Ataque de fabricación**, consistente en que se realice una modificación para conseguir un objeto similar al atacado, de forma que sea difícil distinguir entre el objeto original y el fabricado.

**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 (también existen ataques por modificación)

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

~**~** Equipo que solo puede realizar filtrado de paquetes. **firewall de red.**

~**~** Equipo que crea un canal de comunicación entre cliente y servidor para todo

tipo de aplicación del cliente. **Pasarelas o proxy de aplicación.**

~**~** Equipo que recuerda las comunicaciones iniciadas desde la LAN a internet

para admitir automáticamente los paquetes de respuesta de internet a la

LAN**. Routers**

**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 compartir una dirección IP pública entre todas las

direcciones IP 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.***

1. El bastión es la única parte del firewall conectado a la red interna.
2. Se genera una DMZ entre ambos.
3. Por ultimo sí ambos elementos del firewall, constituyen un punto único de fallo, el diseño incluye dos etapas de protección, lo que en general lo hace más robusto.

**8. Complete la siguiente frase:**

En un *firewall screened host* se emplea un equipo previo al bastión para

realice el filtrado de los paquetes de red, y que está configurado para que solo envíe hacia el

bastión el tráfico de internet filtrado, y para que solo admita conexiones

internas desde el bastion.

**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. Permitir

b. Del servidor bastionado a internet. Permitir

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

d. De los clientes al servidor bastionado. Permitir

**12. Complete la siguiente frase:**

Las redes privadas virtuales permiten disponer de conexiones o canales de comunicación

seguros, empleando redes no seguras o públicas, como

internet, usando para ello métodos criptográficos, que permiten defender

las comunicaciones de ataques de interceptación y de ataques de modificación.

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

**VPN sitio a sitio**: se usa para conectar diferentes oficinas de una misma empresa, que precisen intercambiar datos confidenciales, evitando el alquiler de circuitos dedicados, considerablemente más costosos

**VPN de acceso remoto**: se usa para permitir el teletrabajo sin comprometer la seguridad. Es posible tener acceso de un ordenador a una red, o bien acceso de ordenador a ordenador.

**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.**

**PPTP:** Es uno de los más antiguos, y opera en el nivel de enlace (capa 2 del modelo OSI), de manera que se emplea cifrado nodo a nodo. Se apoya en el protocolo PPP (Point to Point Protocol), y está soportado por sistemas Microsoft Windows, permitiendo a dos ordenadores construir una VPN entre ellos.

**L2TP:** tiene como base PPTP, de manera que también opera en capa 2, y está orientado a comunicaciones nodo a nodo, por lo que se precisa que todos los elementos intermedios cumplan con el protocolo L2TP, que sí es un estándar reconocido por IETF. Emplea autenticación PPP que se realiza entre los puntos finales del túnel, lo que permite una suplantación de identidad por el camino.

**IPsec:** Es un conjunto de protocolos

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

El uso conjunto de firewalls y VPN, para separar la LAN de internet o para separar subredes LAN o dominios lógicos de seguridad internos, completan las salvaguardas que permiten cerrar perfectamente la infraestructura (física y lógica) en torno a los activos contenidos. Como otras contramedidas, se debe monitorizar su eficacia y rendimiento **mediante registros de auditoría** y **verificaciones regulares** de su buen funcionamiento, desconfiando del comportamiento conocido.