**Ejercicios de repaso y autoevaluación. MF0486-3. UD1**

**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. **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 LOS RIESGOS DEL SISTEMA DE INFORMACIÓN y** unas **DIRECTRICES**

**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. **AMENAZA** 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.**

**Preventiva – Recinto estanco**

**Reactiva – Desconexión eléctrica, bombas de achique y desagües.**

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

**Localizar el servidor en una zona segura nunca sobre estancias**

**Control de temperatura**

**Alarmas de detección**

**Puerta Ignífuga**

**Extintores CO2**

**Mobiliario resistente a fuego**

**Paredes de hormigón armado u otro material que resista las altas temperaturas**

**No almacenar materiales inflamables en la sala del CPD**

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

**Restricciones en los puertos USB**

**Antivirus, antimalware, antispyware…**

**Firewall**

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

**La que usa mayúsculas y minúsculas porque admite más combinaciones**

**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.

**Ejercicios de repaso y autoevaluación. MF0486-3. UD2**

**1. Complete la siguiente oración:**

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

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

**Cuáles son los procesos críticos, u ordenarlos por prioridad.**

**Cuál es el daño/impacto, en función del tiempo que se tarde en restablecerse el servicio.**

**Cuál es el coste de las diferentes estrategias de recuperación, que proporcionarán un tiempo y un punto objetivo de recuperación.**

**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 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 **interna** siempre requiere de esta calificación, expresa por el área o responsable de comunicación de la empresa.

c. La información **pública** 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. **ALTO**

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

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. **DISPONIBILIDAD**

b. Si se emplea el más alto. **DISPONIBILIDAD**

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. **INTEGRIDAD**

**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 de la parada**
2. **Coste de las medidas de recuperación**



**Ejercicios de repaso y autoevaluación. MF0486-3. UD3**

**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:**

**Cuando la empresa quiera obtener determinadas certificaciones de cumplimiento de normas (v.g. ISO 27001).**

**Para conducir una auditoría de seguridad, o para definir el marco de cumplimiento de una ley.**

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

**Mitigar el riesgo.**

**Evitar el riesgo.**

**Transferir el riesgo.**

**Aceptar el riesgo.**

**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.**

**Capa 3: la información y los datos.**

**Capa 2: el sistema de información.**

**Capa 1: el entorno que se precisa.**

**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: **Es el impacto en un activo a consecuencia de su valor propio (no del acumulado), y de las amenazas a las que están expuestos sus activos inferiores.**

b. El riesgo acumulado: **Es el riesgo producido por el impacto acumulado de un activo, a raíz de la frecuencia de su amenaza.**

c. El impacto acumulado: **Es el impacto producido sobre el valor acumulado de un activo, a raíz de sus amenazas. Nótese que se emplea su valor total o acumulado, es decir, el procedente de sus activos superiores y el suyo propio.**

d. El riesgo repercutido: **Es el riesgo en un activo a consecuencia de su impacto repercutido, y de la frecuencia de la amenaza.**

**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:**







**1 Coste de las salvaguardas**

**2 Coste del riesgo residual**



**Ejercicios de repaso y autoevaluación. MF0486-3. UD4**

**1. Empareje las 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 qué 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 código 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 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 **principios básicos**  y **requisitos mínimos** para una adeciada S.I.

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

- Identificar los riesgos: **Planificar**

- Tomar medidas preventivas y correctivas: **Corregir**

- Revisar evaluaciones de riesgo: **Medir**

- Definir efectividad controles: **Hacer**

- Analizar y evaluar los riesgos: **Planificar**

- Plan de tratamiento de riesgos: **Hacer**

- Detección y respuesta a incidentes: **Hacer**

- Seleccionar controles para riesgos: **Planificar**

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

**La acción.**

**Los recursos.**

**Las responsabilidades.**

**Las prioridades de la gerencia para manejar los riesgos 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, con referencia al informe de insuficiencias del AR**

**Periodo de ejecución, desde su arranque hasta su puesta en operación**

**Salvaguardas a implantar: se recogen aquí los trabajos de apoyo, la selección de estas salvaguardas frente a otras, detallando:**

**Los escenarios de impacto y riesgo que se tratan**

**Los activos afectados**

**Las amenazas afrontadas**

**La valoración de los activos**

**La valoración de las amenazas**

**Niveles de impacto y riesgo residual una vez queden en operación.**

**Los indicadores de eficacia y eficiencia que permitan conocer en cada momento la calidad del desempeño de la función de seguridad y su función en el tiempo**

**Responsables de la ejecución, deben incluirse parejas “tarea – nombre de responsable final”**

**Estimación de costes financieros, incluyendo:**

**Los costes de adquisición**

**Los de contratación de servicios**

**Los de desarrollo de soluciones llave en mano y las comparaciones entre alternativas**

**Los costes de formación**

**Los de explotación**

**El impacto en la productividad de la e–– Estimación de recursos, que incluya la relación de tareas y actividades a afrontar como:**

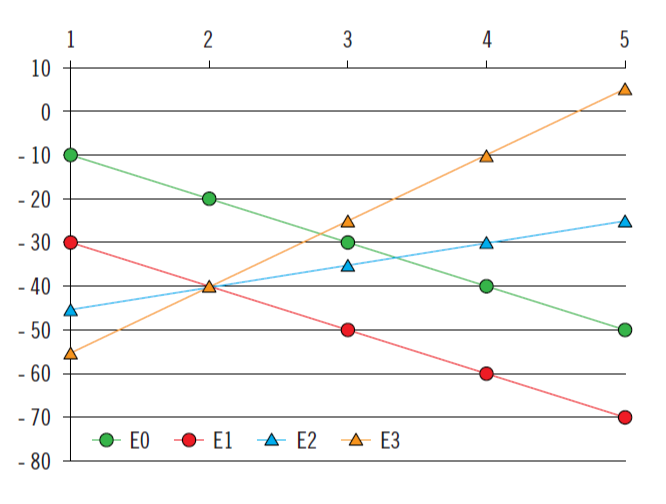
**Cambios de normativa y desarrollo de procedimientos**

**Soluciones técnicas (programas, equipos, comunicaciones, locales)**

**Planes de despliegue**

**Planes de formación**

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



**E3 es el de mayor inversión inicial, se obtiene rentabilidad en**

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

**Ejercicios de repaso y autoevaluación. MF0486-3. UD5**

**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/CE, 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 las 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.

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. **SI**
2. Los datos de Fuerzas y Cuerpos de Seguridad referentes a investigaciones sobre organizaciones terroristas internacionales que puedan operan en España.

**NO**

1. Un listado con los datos de contacto particular de sus conocidos, aficionados a las apuestas deportivas de fútbol, que incluye sus números de cuenta para transferirles los beneficios.

**NO**

**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:**

**Con el previo consentimiento del afectado, para fines directamente relacionados**

**con las funciones legítimas del cedente y del cesionario**

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

**Sin el previo consentimiento del interesado, cuando la cesión esté autorizada**

**en una ley, cuando se trate de datos recogidos de fuentes accesibles**

**al público, cuando el tratamiento responda a una relación jurídica**

**que implique necesariamente la conexión de dicho tratamiento con ficheros**

**de terceros, cuando la comunicación que tenga que efectuarse**

**tenga por destinatario al Defensor del Pueblo, al Ministerio Fiscal, a**

**los Jueces o Tribunales o al Tribunal de Cuentas, cuando la cesión sea**

**entre Administraciones con fines estadísticos, históricos, o científicos, o**

**cuando la cesión de DCP relativos a la salud sea necesaria para solucionar**

**una urgencia, o realizar estudios epidemiológicos.**

**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. **Grave**

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

**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 aplicará ninguna sanción económica; por lo que bastaría inscribirse después.
4. Se rellena el formulario de la agencia en internet, abonando las tasas de inscripción según el nivel de las medidas que se quieran aplicar.

**15. Indique cuáles son las medidas de seguridad que se aplicaría a una base de datos que tuviese un nivel de seguridad básico.**

a. Funciones y obligaciones del personal, registro de incidencias, control acceso, gestión de soportes y documentos, identificación y autenticación, y copias de respaldo y recuperación.

**b. Registro de incidencias, gestión de soportes y documentos, y responsable de seguridad.**

c. Funciones y obligaciones del personal, control de accesos, gestión de soportes, y documentos y auditorías.

d. Funciones y obligaciones del personal, control de accesos, identificación, y autenticación y telecomunicaciones.

**Ejercicios de repaso y autoevaluación. MF0486-3. UD6**

1. **Complete el siguiente párrafo:**

La Seguridad física se ocupa de barreras **físicas**, procedimientos, y **mecanismos** de control, para proteger los activos de las **barreras** 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.**

**Perímetro de seguridad física (9.1.1).**

**Controles físicos de entrada (9.1.2).**

**Seguridad de las oficinas, despachos e instalaciones (9.1.3).**

**Trabajo en áreas seguras (9.1.5).**

**Áreas de acceso público y de carga y descarga (9.1.6).**

**Política de control de acceso (11.1).**

**Gestión del acceso de los usuarios (11.2).**

**Responsabilidades de los usuarios (11.3).**

**Control del acceso a la red (11.4).**

**Control del acceso al sistema operativo (11.5).**

**Control del acceso a las aplicaciones y a la información (11.6).**

**Teletrabajo (11.7).**

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. - **SAI**

b. Caída de rayos. - **Descargadores de gas**

c. Interferencias o ruido eléctrico. - **Filtros**

d. Interrupción prolongada del suministro. - **Generador eléctrico**

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

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

**No debe existir comunicación por suelos ni techos con los recintos cercanos. No deben permitir la entrada de fuego, ni propagarlo si se**

**originara dentro.**

* **Puerta con suficiente grado de protección frente al fuego. No debe permitir la entrada de fuego, ni propagarlo si se originara dentro.**
* **Detectores de humo, que se deben situar en el falso techo, que es donde primero se acumulará el humo. Deberían estar conectadas a una alarma audible, y ser practicables para su mantenimiento.**
* **Alarmas de incendio manuales, localizadas en sitios estratégicos, generalmente cerca de puertas y salidas de emergencia. Deberían estar conectadas a una alarma audible.**
* **Extintores de incendio manuales.**
* **Sistemas de extinción de incendio automático. Estos sistemas se activan de manera automática, cuando detectan una alta temperatura**

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

a. Active Directory (directorio activo). **Identificación**

b. Kerberos. **Autentificación**

c. Login (nombre de usuario). **Autentificación**

d. OpenLDAP.  **Directorio**

1. **Complete la siguiente frase:**

Las **listas** de 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 **xcacls**, y en sistemas Linux, con el comando **chmod.**

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

**Debe incluir números.**

**Utilice una combinación de letras mayúsculas y minúsculas.**

**Incluya caracteres especiales. ¿Cuáles son los caracteres especiales?**

**Cualquiera de los siguientes caracteres: - \* ? ! @ # $ / () {} = . , ; :**

**Tenga una longitud mayor o igual a 6 caracteres**

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.**

**Política sobre el uso de los servicios de red.**

**Autenticación de usuario para los usuarios remotos, o conexiones externas**

**Identificación del equipo automática**

**Protección de puertos de diagnóstico y configuración remota**

**queeeSegregación de redes**

1. **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 el usuario conoce: una contraseña**

**Algo que el usuario posee: una tarjeta inteligente o smartcard**

**Algo que el usuario es: sistemas biométricos**

**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