Solucionario de

ejercicios de autoevaluación

Ejercicios de autoevaluación
Unidad de Aprendizaje 1

1. **Indica si la siguiente afirmación es verdadera o falsa: "La seguridad informática trata de dar una visión integral que permita a la empresa identificar, detectar, predecir y reaccionar a los riesgos inherentes por el uso de tanto volumen de información".**

   - **Verdadero**
   - Falso

2. **Deben cumplir un mínimo de exigencias para garantizar la seguridad en el uso de la información...**

   a. ... los responsables de la seguridad.
   b. ... toda organización al completo, colaboradores y usuarios autorizados.
   c. ... los gerentes y responsables de cada departamento.
   d. ... toda organización al completo, colaboradores, usuarios autorizados y también los no autorizados.

3. **La encargada de velar por el cumplimiento de las obligaciones, dar difusión de las medidas impuestas, los riesgos expuestos y realizar tantas revisiones como sean necesarias para mantener activa la estrategia de seguridad en la gestión de la información, es...**

   a. ... la gerencia.
   b. ... la política de seguridad.
   c. ... la sección especializada en seguridad.
   d. ... cada dependencia o área empresarial.

4. **Los pilares básicos de la información interna son:**

   a. La integridad y confidencialidad.
   b. La confidencialidad, integridad y disponibilidad.
   c. La disponibilidad y la integridad.
   d. La disponibilidad y confidencialidad.

5. La política de seguridad debe conseguir...

a. ... que todas las personas que conforman una empresa sepan distinguir una información pública de una información confidencial.
b. ... que todas las personas que conforman una empresa sepan distinguir una información restringida de una información confidencial.
c. ... que todas las personas que conforman una empresa sepan distinguir una información pública de una información restringida.
d. ... que todas las personas que conforman una empresa sepan y distingan cuál es la información crítica de su organización.

6. Un *hacker* es:

a. Un ciberdelincuente.
b. Un profesional informático o con altos conocimientos en informática que hace vulnerable los sistemas de información de las organizaciones, accediendo a ellos ilegalmente y siendo capaz de manipularlos parcialmente o en su totalidad.
c. Un profesional informático o con altos conocimientos en informática que hace vulnerable los sistemas de información de las organizaciones, accediendo a ellos legal o ilegalmente y siendo capaz de manipularlos parcialmente o en su totalidad.
d. Un profesional informático o con altos conocimientos en informática que hace vulnerable los sistemas de información de las organizaciones, accediendo a ellos legalmente y siendo capaz de manipularlos parcialmente o en su totalidad.

7. Hablar de un *keylogger* es:

a. Hablar de un tipo de *software* cuya tecnología copia las pulsaciones de los usuarios, de esta manera puede descifrar contraseñas haciendo un uso indebido.
b. Hablar de una de las amenazas para los sistemas de seguridad de la información.
c. Hablar de una práctica utilizada por los piratas informáticos capaz de robar información crítica.
d. Todas las opciones son correctas.

8. Un árbol de ataque es:

a. Un tipo de vulnerabilidad del sistema informático.
b. Un virus informático.
c. Una técnica de análisis muy efectiva para crear un patrón de posibles entradas de ataques deliberados al sistema de información, de alguna manera identifica previamente los pasos, fases o secuencias que realizaría un posible atacante si decidiera actuar.
d. Todas las opciones son correctas.

9. Para aumentar las posibilidades de evitar contagios y vulnerabilidades es importante...

a. ... mantener actualizado el sistema informático.
b. ... contar con un cortafuego.
c. ... tener conocimiento de los riesgos y amenazas.
d. Todas las opciones son correctas.

10. En cuanto a la seguridad Red...

a. ... solo es necesario instalar en servidores aquello estrictamente necesario.
b. ... no olvides tener copias de seguridad.
c. ... no se puede obtener un pronóstico certero al 100 %.
d. Todas las opciones son incorrectas.

Ejercicios de autoevaluación Unidad de Aprendizaje 2

1. **Indica si la siguiente afirmación es verdadera o falsa: "La política de seguridad informática hace referencia a los requisitos generales de un sistema de información en el que se define qué está permitido y qué no en el ámbito de seguridad informática de una empresa".**

   - **Verdadero**
   - Falso

2. **El fundamento de toda política de seguridad...**

   a. ... es identificar a los responsables de la seguridad en la empresa.
   b. ... trata de evitar, prevenir y gestionar que las tecnologías mediante su uso inadecuado deje las puertas abiertas a la ciberdelincuencia, pudiendo *hackear,* controlar, manipular o desestabilizar el sistema operativo de cualquier empresa, negocio u organización.
   c. ... persigue garantizar al 100 % la seguridad informática y de la información.
   d. Todas las opcion**es son correctas.**

3. **La seguridad informática...**

   a. ... centra su atención exclusivamente en prevenir ataques y proteger información.
   b. ... no solo centra su atención en prevenir ataques y proteger información, también está orientada a transmitir conciencia y responsabilidad en todos aquellos usuarios que diariamente manejan en sus empresas equipos informáticos e información crítica.
   c. ... centra su atención exclusivamente en transmitir conciencia y responsabilidad en todos aquellos usuarios que diariamente manejan en sus empresas equipos informáticos e información crítica.
   d. ... centra su atención en registrar elementos técnicos que evitan riesgos innecesarios en el manejo de información.

4. Los principales motivos por los que una empresa o negocio debe tener una política de seguridad son:

a. Proteger a los usuarios.
b. Proteger equipos e infraestructuras.
c. Proteger equipos e infraestructuras, proteger a los usuarios y proteger la información.
d. Proteger la información.

5. La política de seguridad debe conseguir...

a. ... que todos los elementos de una organización sean seguros.
b. ... que todas las personas que conforman una empresa conozcan las consecuencias del incumplimiento de las normas relativas a la seguridad.
c. ... que el sistema informático de una empresa tenga sus equipos actualizados.
d. ... que todas las personas que conforman una empresa sepan y distingan cuál es la información crítica de su organización.

6. La base del diseño de una política de seguridad informática debe ser:

a. Atemporal y holística.
b. Atemporal y adaptada.
c. Holística y atemporal.
d. Holística, adaptada y atemporal.

7. La política de seguridad...

a. ... tiene carácter genérico y normativo.
b. ... debe identificar las contraseñas de acceso a la información.
c. ... debe reflejar la filosofía de la empresa, donde queda integrada el afán y la motivación entre los colaboradores por proteger activamente todos los bienes y valores que la conforman, y nunca desde la contención y el ánimo de sancionar.
d. Todas las opciones son correctas.

8. Algunas de las acciones para conformar una política de seguridad son:

a. Realizar seguimientos de transacciones y operativas diarias para adaptar las políticas frente a cambios inesperados.
b. Determinar en cada departamento a los responsables de seguridad de su sección.
c. Realizar reuniones de consenso con los responsables de departamento para definir políticas de seguridad.
d. Todas las opciones son correctas.

9. Para que se cumplan las decisiones sobre estrategias y políticas...

a. ... es necesario implicar al personal desde la responsabilidad individual.
b. ... es necesario concienciar y comprometer al personal.
c. ... es necesario que el personal comprenda el porqué de estas decisiones.
d. Todas las opciones son correctas.

10. El Reglamento General de Protección de datos...

a. ... es de obligado cumplimiento.
b. ... establece las medidas de protección de datos personales en las empresas.
c. ... es una normativa a nivel europeo.
d. Todas las opciones son correctas.

Ejercicios de autoevaluación Unidad de Aprendizaje 3

1. **La razón principal de proceder a realizar una auditoría informática es:**

    a. Identificar responsabilidades frente a las incidencias surgidas.
    b. Obtener información manifiesta del estado del sistema de información y detectar fallos y vulnerabilidades.
    c. Sancionar por el incumplimiento de la norma.
    d. No tiene un objetivo concreto.

2. **La auditoría de la seguridad del sistema informático y de la gestión de seguridad de la información es el conjunto de medidas y procedimientos que permiten conocer la situación de los activos de la información de una organización, empresa o negocio, gracias a las acciones de:**

    a. Protección y medición.
    b. Medición y control.
    c. Protección y control.
    d. Protección, control y medición.

3. **El ciclo del sistema de gestión de seguridad de la información...**

    a. ... es un ciclo cerrado que controla si se dan los requerimientos de seguridad.
    b. ... es un ciclo abierto que controla si se dan los requerimientos de seguridad.
    c. ... es un ciclo cerrado que no controla si se dan los requerimientos de seguridad
    d. ... es un ciclo abierto que no controla si se dan los requerimientos de seguridad.

4. **Las incidencias detectadas en un informe de auditoría se formularán en base y en el orden siguiente:**

    a. Requisito, evidencia y problema.
    b. Evidencia, requisito y problema.

c. Problema, requisito y evidencia.
d. Problema, evidencia y requisito.

5. La acción auditora está asociada a los principios de:

a. Evaluación y control.
b. Evaluación y mejora.
c. Evaluación, control y mejora.
d. Control y mejora.

6. La seguridad de la información reúne los principios de:

a. Confidencialidad, Integridad y Coherencia.
b. Confidencialidad, Intencionalidad y Disponibilidad.
c. Confidencialidad, Integridad y Disponibilidad.
d. Confidencialidad, Integridad y Permanencia.

7. La Norma internacional ISO que acredita a la empresa de reunir los principios de confidencialidad, integridad y disponibilidad es:

a. Norma ISO 27002
b. Norma ISO 27004
c. Norma ISO 27001
d. Norma ISO 21000

8. Uno de los requisitos que persigue un plan de seguridad es:

a. Mejora continua.
b. Informar al organismo superior de control.
c. Mejorar definitivamente los aspectos de seguridad de la empresa.
d. Todas las opciones son incorrectas.

9. Los activos de la información son:

a. El conjunto de recursos de información.
b. El conjunto de recursos de físicos.
c. El conjunto de recursos tecnológicos y servicios.
d. Todas las opciones son correctas.

10. El sobrecalentamiento de los equipos informáticos por falta de ventilación es:

a. Un área de mejora de la seguridad humana.
b. Un área de mejora de la seguridad física.
c. Un área de mejora de la seguridad del entorno.
d. Todas las opciones son correctas.

Ejercicios de autoevaluación
Unidad de Aprendizaje 4

1. **Determina si la siguiente oración es verdadera o falsa: "El término estrategia de seguridad hace referencia al diseño del conjunto de acciones y el establecimiento de medidas para que su puesta en marcha dé respuesta a facilitar la consecución de un objetivo de protección".**

   - **Verdadero**
   - Falso

2. **Las funcionalidades de una estrategia de seguridad son:**

   a. Conocer los métodos y recursos usados por los atacantes.
   b. Establecer medidas preventivas.
   c. Realizar simulaciones de ataques y responder a eventualidades.
   d. Todas las opciones son correctas.

3. **La estrategia de menor privilegio es aquella cuyo objetivo es:**

   a. Conceder los mismos permisos a todos los usuarios.
   b. Definir complejas contraseñas de usuarios para proteger los accesos.
   c. Bloquear accesos.
   d. Disminuir la exposición a los ciberdelincuentes.

4. **La defensa en profundidad es:**

   a. Aquella estrategia de seguridad cuya metodología aplicada es la de establecer diferentes líneas de defensa, que facilite ataques informáticos para ser analizados.
   b. Aquella estrategia de seguridad cuya metodología aplicada es la de establecer una única línea de defensa, que dificulte mediante ataques informáticos el acceso indebido y no autorizado a los sistemas de información.

c. Aquella estrategia de seguridad cuya metodología aplicada es la de establecer diferentes líneas de defensa, que dificulte mediante ataques informáticos el acceso indebido y no autorizado a los sistemas de información.
d. Una estrategia básica de seguridad informática.

5. La estrategia punto de choque...

a. ... es el procedimiento que utiliza como medida de protección el establecer una única vía de entrada al sistema informático, de tal manera que también sea la una única puerta de acceso de intrusos.
b. ... es el procedimiento que utiliza como medida de protección el establecer varias vías de entrada al sistema informático, de tal manera que puedan aplicarse métodos de protección diversos.
c. ... es una estrategia que bloquea el sistema cuando detecta un intruso.
d. Todas las opciones son incorrectas.

6. El eslabón más débil de la cadena de seguridad son:

a. Los dispositivos móviles.
b. Las redes wifi abiertas.
c. Los ordenadores desactualizados.
d. Las personas.

7. Cuando se interrumpe el funcionamiento del sistema o este se bloquea, es una medida de protección de la estrategia de seguridad...

a. ... del eslabón más débil.
b. ... de menor privilegio.
c. ... de postura de fallo seguro.
d. ... del punto de choque.

8. La postura de negación establecida responde al principio de:

a. "Aquello que no está prohibido expresamente, está permitido".
b. "Aquello que está prohibido expresamente, no está permitido".

c. "Aquello que no está permitido, no está prohibido".
d. Todas las opciones son incorrectas.

9. Generar conciencia colectiva de seguridad en la empresa es:

a. El objetivo de la estrategia de simplicidad.
b. El objetivo de la estrategia de diversificación de la defensa.
c. El objetivo de la estrategia de participación universal.
d. Todas las opciones son incorrectas.

10. Un sistema de almacenamiento tradicional...

a. ... implica una sencilla manera de almacenar la información.
b. ... implica una compleja manera de organizar la información.
c. ... es una estrategia que debería seguir aplicándose.
d. ... es una estrategia compleja y segura.

Ejercicios de autoevaluación Unidad de Aprendizaje 5

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. La interconectividad de los ordenadores mediante canales de transmisión hace posible el transporte de datos y de información.

- **Verdadero**
- Falso

b. El entorno red es aquel espacio exclusivamente físico que engloba el contexto donde quedan interconectados los equipos informáticos, a través del cual pueden intercambiar información y recursos.

- Verdadero
- **Falso**

c. Los medios o canales de transmisión de señales de datos pueden ser de dos tipos: alámbricos (WiFi) o inalámbrico (Enthernet).

- Verdadero
- **Falso**

2. El área de influencia de la red WPAN es:

a. Local.
b. Mundial.
c. Metropolitana.
d. Exclusiva para dispositivos cercanos.

3. Las empresas actuales confieren mayor garantía a la conexión...

a. ... inalámbrica frente al cableado.
b. ... alámbrica frente a la inalámbrica.
c. ... híbrida.
d. Todas las opciones son incorrectas.

4. Una red corporativa libre de cables implica...

a. ... un esfuerzo para generar consciencia corporativa de seguridad informática entre todos los empleados que configuran la organización, con el fin de evitar riesgos innecesarios por el uso de dispositivos móviles en el desempeño profesional.
b. ... mayor productividad.
c. ... mayor eficiencia.
d. Todas las opciones son correctas.

5. Un sistema operativo red es:

a. Un *software* que permite la desconexión de equipos informáticos (servidores, equipos y dominios) que conforman una red de ordenadores.
b. Un *hardware* que permite la interconexión de equipos informáticos (servidores, equipos y dominios) que dan acceso a los recursos *(hardware* y *software),* creando redes de ordenadores.
c. Un *software* que permite la interconexión de equipos informáticos (servidores, equipos y dominios) que dan acceso a los recursos *(hardware* y *software),* creando redes de ordenadores.
d. Todas las opciones son incorrectas.

6. El inventario red es:

a. Un *hardware.*
b. Un *software.*
c. Un conjunto de acciones.
d. Todas las opciones son incorrectas.

7. NMAP es:

a. Una herramienta de auditoría de seguridad red.
b. Una herramienta de código abierto.
c. Una herramienta que evalúa y valora la seguridad del sistema informático de la empresa.
d. Todas las opciones son correctas.

8. El orden de las fases de un ataque informático es:

a. Reconocimiento, escanear, acceder, mantener el acceso y eliminar la evidencia.
b. Reconocimiento, escanear, acceder, eliminar la evidencia y mantener el acceso.
c. Reconocimiento, acceder, escanear, mantener el acceso y eliminar la evidencia.
d. Reconocimiento, acceder, mantener el acceso, escanear y eliminar la evidencia.

9. El test de intrusión es:

a. Una actitud proactiva y acción exclusiva de la empresa como medida de seguridad informática.
b. Una actitud reactiva y acción exclusiva de la empresa como medida de seguridad informática.
c. Una actitud proactiva de la empresa como medida de seguridad informática.
d. Una actitud reactiva de la empresa como medida de seguridad informática.

10. El reporte final de una auditoria red debe contemplar:

a. Un resumen de las pruebas realizadas y los resultados obtenidos, además del detalle de cada prueba y el objetivo que persigue.
b. Los resultados del test de intrusión con la descripción detallada de cada análisis y maniobras realizadas para cada vulnerabilidad detectada.
c. La relación de consejos y recomendaciones para solucionar problemas detectados, además de la categorización de importancia de cada problema de seguridad encontrado para establecer prioridades.
d. Todas las opciones son correctas.

Ejercicios de autoevaluación
Unidad de Aprendizaje 6

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Los instigadores de ataques informáticos aprovechan la gran complejidad del entramado empresarial actual para ejecutar sus acciones.

- **Verdadero**
- Falso

b. Los ataques necesitan de conexión a internet para llevar a cabo sus propósitos.

- Verdadero
- **Falso**

c. Los ataques pueden clasificarse como ataques locales o remotos

- **Verdadero**
- Falso

2. La ingeniería social es considerada en seguridad informática como la técnica...

a. ... local.
b. ... remota.
c. ... del eslabón más débil.
d. Todas las opciones son incorrectas.

3. El análisis de seguridad de una estación de trabajo se realiza en el siguiente orden:

a. Arranque, contraseñas, permisos y privilegios, redes, comunicación y cortafuegos.
b. Arranque, contraseñas, permisos y privilegios, redes, cortafuegos y comunicación.

c. Arranque, contraseñas, permisos y privilegios, cortafuegos, redes y comunicación.
d. Arranque, contraseñas, redes, permisos y privilegios, cortafuegos y comunicación.

4. En función del objetivo, un ataque puede clasificarse como:

a. Local o remoto.
b. Pasivo o activo.
c. Fuerte o débil.
d. Todas las opciones son correctas.

5. El sistema operativo *UNIX* es:

a. Multidisciplinar.
b. De código abierto.
c. El padre de otros sistemas operativos
d. Todas las opciones son incorrectas.

6. Los servicios red inseguros son:

a. Aquella categoría de servicios que para acceder a ellos no requieren de nombre de usuario ni contraseña.
b. Aquella categoría de servicios que para acceder a ellos requieren de nombre de usuario y contraseña sin encriptar (ocultar datos bajo una clave), con idea de poder ser autentificado y conseguir el acceso.
c. Aquella categoría de servicios que para acceder a ellos requieren de nombre de usuario y contraseña encriptada.
d. Todas las opciones son incorrectas.

7. En el sistema *Unix*...

a. ... las maniobras de encriptación de datos no son reversibles, lo que significa que es imposible dejar las claves de acceso sin encriptar, convirtiendo los servicios a los que se accede totalmente seguros.
b. ... las maniobras de encriptación de datos son irreversibles, lo que significa que es posible dejar las claves de acceso sin encriptar, convirtiendo los servicios a los que se accede totalmente vulnerables e inseguros.

c. ... las maniobras de encriptación de datos son reversibles, lo que significa que es posible dejar las claves de acceso sin encriptar, convirtiendo los servicios a los que se accede totalmente vulnerables e inseguros.
d. Todas las opciones son incorrectas.

8. Cuando hablamos de amenazas, ¿se hace referencia a la posibilidad de sufrir un riesgo ocasionado siempre por un pirata informático?

a. No, no siempre el riesgo de sufrir una pérdida o sustracción de información proviene de la acción intencionada de un intruso.
b. Sí, tiene que darse la acción intencionada del intruso.
c. En la gran mayoría de las ocasiones las amenazas son por catástrofes naturales.
d. Todas las opciones son incorrectas.

9. Un sistema operativo seguro deberá estar diseñado para:

a. Evitar pérdida de datos, controlar la privacidad del usuario y controlar los accesos.
b. Evitar pérdida de datos, controlar la privacidad de los clientes y de los proveedores.
c. Controlar la privacidad de la información y los accesos a esta.
d. Evitar pérdida de datos, controlar la privacidad de la información y los accesos a esta.

10. Un plan de actuación frente a ataques debe contemplar:

a. Medidas técnicas, organizativas, de recuperación y de respuesta.
b. Medidas técnicas, organizativas, legales y de respuesta.
c. Medidas técnicas, legales, de recuperación, de respuesta y medidas complementarias.
d. Medidas técnicas, organizativas, legales, de recuperación, de respuesta y medidas complementarias.

Ejercicios de autoevaluación
Unidad de Aprendizaje 7

1. Indica si las siguientes afirmaciones son verdaderas o falsas.

a. Actualmente, es imposible concebir un entorno global de conexión, ya sea como usuario o como empresa, sin la existencia de una infraestructura inalámbrica que los respalde.

- **Verdadero**
- Falso

b. Todo el mundo conoce cómo funciona una red inalámbrica.

- Verdadero
- **Falso**

c. La red inalámbrica también se denomina *Wireless Network.*

- **Verdadero**
- Falso

2. La red inalámbrica es:

a. Un concepto que viene a describir la habilitación mediante conexión del punto de intersección (nodos) entre instrumentos informáticos básicos que quedan desconectados mediante ondas electromagnéticas, que no requieren cables ni conexión alámbrica y mediante la cual es posible la transferencia y recepción de datos.
b. Un concepto que viene a describir la inhabilitación mediante conexión del punto de intersección (nodos) entre instrumentos informáticos básicos que quedan conectados mediante ondas electromagnéticas, que no requieren cables ni conexión alámbrica y mediante la cual es posible la transferencia y recepción de datos.

c. Un concepto que viene a describir la habilitación mediante conexión del punto de intersección (nodos) entre instrumentos informáticos básicos que quedan conectados mediante ondas electromagnéticas, que no requieren cables ni conexión alámbrica y mediante la cual es posible la transferencia y recepción de datos.
d. Todas las opciones son incorrectas.

3. La red inalámbrica circula gracias a las ondas...

a. ... electrónicas.
b. ... magnéticas.
c. ... electromagnéticas.
d. Todas las opciones son incorrectas.

4. Gracias al estudio del espectro electromagnético es posible...

a. ... oír las ondas electromagnéticas.
b. ... ver las ondas electromagnéticas.
c. ... obtener información específica acerca de las propiedades físicas de los objetos.
d. Todas las opciones son correctas.

5. Las redes inalámbricas no son...

a. ... más económicas que una red alámbrica.
b. ... más accesibles que una red alámbrica.
c. ... más segura que una red alámbrica
d. Todas las opciones son correctas.

6. La Norma estándar IEEE 802.11 es:

a. La versión más nueva de la norma estándar original.
b. La norma estándar original de las redes inalámbricas.
c. La norma estándar original de las redes alámbricas.
d. Todas las opciones son incorrectas.

7. El modelo OSI acorde al diseño estándar de la norma 802.11 consta de las siguientes capas:

a. Capa física, de enlace, de red, de transporte, de sesión y de presentación.
b. Capa física, de enlace, de red, de transporte y de sesión.
c. Capa física, de enlace, de red, de transporte, de sesión y de aplicación.
d. Capa física, de enlace, de red, de transporte, de sesión, de presentación y de aplicación.

8. El protocolo WEP integra...

a. ... la encriptación.
b. ... la autenticación.
c. ... la autenticación y la encriptación.
d. Todas las opciones son incorrectas.

9. La autenticación wep implica...

a. ... conectarse a un sistema abierto.
b. ... conectarse con una clave compartida.
c. ... conexión por algunas de las dos técnicas: sistema abierto o clave compartida.
d. Todas las opciones son incorrectas.

10. Otros mecanismos de cifrado alternativo a wep son:

a. WPA y WPA2.
b. WPA y WPA3.
c. WPA2 y WPA3.
d. WPA, WPA2, WPA3, TKIP y AES.

Ejercicios de autoevaluación
Unidad de Aprendizaje 8

1. **Indica si la siguiente afirmación es verdadera o falsa: "Hoy en día, ya es posible entender la seguridad informática sin tener en cuenta las aplicaciones prácticas de la criptografía y el criptoanálisis".**

   - **Verdadero**
   - Falso

2. **Uno de las aplicaciones prácticas más comunes de las técnicas criptográficas está en...**

   a. ... el ámbito militar.
   b. ... el ámbito empresarial.
   c. ... el ámbito privado.
   d. Todas las opciones son correctas.

3. **La criptografía dota a los actuales sistemas de informática y de la información...**

   a. ... de privacidad.
   b. ... de confidencialidad y seguridad.
   c. ... de privacidad, confidencialidad y seguridad.
   d. Todas las opciones son incorrectas.

4. **El uso que la población hace de internet...**

   a. ... hace que sean necesarios los aportes de la criptografía para dar mayor fiabilidad a todos los procesos de transmisión y recepción de datos.
   b. ... hace que sea necesario que todos los usuarios de internet sepan aplicar las técnicas y procedimientos criptográficos.
   c. ... hace que no sea necesario que se conozcan y descubran técnicas de criptoanálisis.
   d. Todas las opciones son correctas.

5. El conjunto de mecanismos o procedimientos que comprende la esencia de privacidad, confidencialidad y seguridad de la información, queda englobado en las maniobras de...

a. ... cifrado.
b. ... descifrado.
c. ... cifrado y descifrado.
d. Todas las opciones son incorrectas.

6. El algoritmo criptográfico es:

a. El mecanismo que transforma los datos finales en un mensaje descifrado.
b. El mecanismo que transforma los datos originales en un mensaje cifrado.
c. Una serie de movimientos lógicos y encadenados que llevan a descifrar mensajes en clave.
d. Todas las opciones son incorrectas.

7. El procedimiento criptográfico a través del cual se utiliza una misma clave para cifrar y descifrar, siendo necesario que tanto el emisor del mensaje como el receptor sepan de antemano esa clave, se denomina:

a. Criptografía asimétrica.
b. Criptografía simétrica.
c. Algoritmo criptográfico.
d. Todas las opciones son incorrectas.

8. El principio por el cual se pretende evitar o detectar ataques criptográficos, utilizando el uso reiterado de códigos en los mensajes transmitidos se denomina:

a. Temporalidad
b. Confidencialidad
c. Integridad
d. Redundancia

9. Las técnicas de sustitución y transposición corresponden a...

a. ... la criptografía moderna.
b. ... el relleno de una sola vez.
c. ... la criptografía clásica.
d. Todas las opciones son incorrectas.

10. Aquellos algoritmos más seguros pero cuyo cálculo es mucho más lento que las utilizadas por las claves simétricas se denominan:

a. Claves públicas.
b. Claves privadas.
c. Firma digital.
d. Todas las opciones son incorrectas.

Ejercicios de autoevaluación
Unidad de Aprendizaje 9

1. **Determina si la siguiente oración es verdadera o falsa: "La autenticación es un mecanismo muy relacionado con la seguridad informática y de la información, tanto es así que desde un punto de vista empresarial sirve de control para determinar los usuarios que acceden a todos o algunos de los recursos de la organización".**

    - **Verdadero**
    - Falso

2. **Los objetivos que persigue una empresa cuando exige un sistema de autenticación de usuarios son:**

    a. Evitar el acceso no autorizado y aportar seguridad en la conexión.
    b. Generar conciencia frente a la seguridad informática y aumentar la protección.
    c. Controlar la huella digital que deja los usuarios y proteger el acceso de dispositivos corporativos.
    d. Todas las opciones son correctas.

3. **Una manera eficaz de proteger el sistema informático de la empresa frente al impacto nocivo que puede ocasionar el robo de información es:**

    a. Adoptar una actitud reactiva en dejar establecidos protocolos de autenticación de usuarios en el acceso a redes corporativas.
    b. Adoptar una actitud proactiva en dejar establecidos protocolos de autenticación de usuarios en el acceso a redes corporativas.
    c. Adoptar una actitud pasiva en dejar establecidos protocolos de autenticación de usuarios en el acceso a redes corporativas.
    d. Todas las opciones son incorrectas.

4. La empresa debe diseñar un sistema red que...

a. ... ofrezca en todo momento información sobre los usuarios que acceden a ella
b. ... ofrezca en todo momento información sobre los usuarios que acceden a ella, pero que además dé atributos de uso.
c. ... ofrezca en todo momento información sobre los usuarios que acceden a ella, pero que además dé atributos de uso y acceso a la red corporativa a cada uno de los usuarios.
d. Todas las opciones son incorrectas.

5. La acreditación de usuario como proceso de validación permitirá acceder a la red de información de la compañía y vendrá determinada por los siguientes pasos previos y en este orden:

a. Autenticación, auditoría y autorización.
b. Autorización, autenticación y auditoría.
c. Auditoría, autenticación y autorización.
d. Autenticación, autorización y auditoría.

6. El proceso de validación es:

a. El paso medio al establecimiento de un vínculo de conexión entre dos identidades (usuarios o máquinas) en el que se acuerda una clave de sesión.
b. El paso último tras el establecimiento de un vínculo de conexión entre dos identidades (usuarios o máquinas) en el que se acuerda una clave de sesión
c. El paso anterior al establecimiento de un vínculo de conexión entre dos identidades (usuarios o máquinas) en el que se acuerda una clave de sesión.
d. Todas las opciones son incorrectas.

7. El protocolo de autenticación se activa...

a. ... en el momento del establecimiento de la conexión entre las dos identidades.
b. ... en el momento posterior al establecimiento de la conexión entre las dos identidades.

c. ... en el momento anterior al establecimiento de la conexión entre las dos identidades.
d. Todas las opciones son incorrectas.

8. El protocolo denominado clave secreta compartida es aquel que:

a. Permite la comunicación entre dos entidades que no han tenido relación previa y que se comunican anónimamente en un entorno no seguro, mediante un establecimiento de una clave que no requiere de autenticación.
b. Se vale del centro de distribución de claves para establecer comunicación con otra identidad de integridad.
c. Se realiza por medio de un KDC ofreciendo autenticación y facilitando una clave de sesión para que dos usuarios puedan comunicarse con una clave privada.
d. Permite la comunicación entre dos entidades gracias a que ambas disponen de una misma clave secreta anterior al proceso de autenticación.

9. El protocolo IKE es aquel que...

a. ... se encarga de proporcionar al IPSEC los principios de confidencialidad, autenticación y de integridad.
b. ... se encarga de manera automática del pacto entre los partícipes de la comunicación, para generar y gestionar las claves para poder establecer la conexión entre AH y ESP.
c. ... es el encargado de proporcionar al IPSEC los principios de integridad (el mensaje no está modificado), autenticación (el emisor del mensaje es quien dice ser) y de no repudio (el emisor del mensaje no puede negar haber enviado el mensaje al receptor una vez realizado).
d. Todas las opciones son incorrectas.

10. El objetivo del protocolo Kerberos es:

a. El de poder contar con servidores lo suficientemente preparados para delimitar el acceso únicamente a usuarios que dispongan de autorización y posibilitar así la autenticación de peticiones de acceso a determinados servicios.
b. Ofrecer un protocolo de interbloqueo para frustrar un ataque.

c. Ofrecer un certificado digital.
d. Todas las opciones son incorrectas.