Pregunta **1**

Correcta

Se puntúa 1,00 sobre 1,00

Salvaguarda es

a. Ninguna de ellas

b. Todo dispositivo capaz de reducir el riesgo ✔

c. Una medida del daño producido

d. La imposibilidad de que se produzca un impacto

La respuesta correcta es: Todo dispositivo capaz de reducir el riesgo

Pregunta **2**

Correcta

Se puntúa 1,00 sobre 1,00

¿Mantener las copias de respaldo de datos externos es un ejemplo de qué tipo de control de recuperación tras un desastre?

a. Control correctivo de archivos

b. Control de transmisión

c. Control preventivo ✔

d. Control de detección

La respuesta correcta es: Control preventivo

Pregunta **3**

Correcta

Se puntúa 1,00 sobre 1,00

Se dice que el hash h(M) de un mensaje M cumple la propiedad de unidireccionalidad,

a. Si conocido un resumen h(M), debe ser computacionalmente imposible encontrar el mensaje M que lo genera. ✔

b. Si es computacionalmente difícil que, conocido M, se encuentre un M' tal que h(M) = h(M').

c. Si h(M) es una función compleja de todos los bits del mensaje M.

d. Si a partir de un mensaje M de cualquier longitud, el resumen h(M) debe tener una longitud fija.

La respuesta correcta es: Si conocido un resumen h(M), debe ser computacionalmente imposible encontrar el mensaje M que lo genera.

Pregunta **4**

Correcta

Se puntúa 1,00 sobre 1,00

La confidencialidad

a. garantiza que la información sólo pueda ser alterada por las personas autorizadas o los usuarios legítimos.
b. garantiza la identidad de los participantes en una comunicación.
c. asegura que la información sólo sea accesible para los usuarios legítimos cuando la necesiten.
d. garantiza que la información sólo sea accesible e interpretada por personas o sistemas autorizados. ✔

La respuesta correcta es: garantiza que la información sólo sea accesible e interpretada por personas o sistemas autorizados.

Pregunta **5**

Correcta

Se puntúa 1,00 sobre 1,00

Un sistema de autenticación que combine el conocimiento de una contraseña y la posesión de un móvil se denomina...

a. Multimedia
b. Multifactor ✔
c. Multiseguro
d. Multipropósito

La respuesta correcta es: Multifactor

Pregunta **6**

Sin contestar

Puntúa como 1,00

La definición de integridad de la información es una cualidad que admite muchos sinónimos en función del contexto en que se aplique. Aun así, en general, entendemos que la información preserva su integridad...

a. cuando preserva la semántica original de la información contenida en el mensaje.
b. cuando puede modificarse, pero sólo a través de copias autorizadas por la política de seguridad.
c. cuando no se modifica.
d. cuando sólo se modifica conforme a la política de seguridad del sistema.

La respuesta correcta es: cuando sólo se modifica conforme a la política de seguridad del sistema.

Pregunta **7**
Correcta
Se puntúa 1,00 sobre 1,00

En la teoría del Análisis de Riesgos, una salvaguarda es

- a. Todo dispositivo capaz de reducir el riesgo. ✔
- b. La imposibilidad de que se produzca un impacto.
- c. Un evento que no desencadena incidentes.
- d. Una medida del daño no producido.

La respuesta correcta es: Todo dispositivo capaz de reducir el riesgo.

Pregunta **8**
Correcta
Se puntúa 1,00 sobre 1,00

De los tres grandes grupos de medidas de seguridad que conocemos, el que una organización coloque en sus instalaciones un cartel de "Cuidado con el perro" podemos incluirla en el grupo de medidas de...

- a. Defensa.
- b. Detección.
- c. Disuasión. ✔
- d. Prevención.

La respuesta correcta es: Disuasión.

Pregunta **9**
Incorrecta
Se puntúa -0,33 sobre 1,00

Los objetivos de seguridad de la información son garantizar:

- a. Tolerancia a fallos, disponibilidad y confidencialidad.
- b. Confidencialidad, disponibilidad y responsabilidad.
- c. Confidencialidad, no repudio y disponibilidad. ✖
- d. Confidencialidad, disponibilidad e integridad.

La respuesta correcta es: Confidencialidad, disponibilidad e integridad.

Pregunta **10**

Correcta

Se puntúa 1,00 sobre 1,00

Indique cuál de las siguientes afirmaciones acerca del protocolo de acuerdo de claves Diffie-Hellman es cierta:

- a. Permite acordar una clave criptográfica entre dos partes y a través de un canal inseguro sin necesidad de intercambiar previamente ningún secreto. ✔
- b. Permite establecer un canal autenticado y cifrado.
- c. Se basa en el esquema de cifrado asimétrico ElGamal.
- d. Necesita intercambiar un secreto entre dos partes, por lo que es susceptible a ataques de escucha en el canal.

La respuesta correcta es: Permite acordar una clave criptográfica entre dos partes y a través de un canal inseguro sin necesidad de intercambiar previamente ningún secreto.

Pregunta **11**

Incorrecta

Se puntúa -0,33 sobre 1,00

Podemos considerar que contratar un seguro es un ejemplo de:

- a. Transferir el riesgo
- b. Eludir el riesgo
- c. Aceptar el riesgo ✖
- d. Mitigar el riesgo

La respuesta correcta es: Transferir el riesgo

Pregunta **12**

Correcta

Se puntúa 1,00 sobre 1,00

El concepto de ataque siempre conlleva la característica de intencionalidad. En los términos más generales, su finalidad es...

- a. hacerse con información confidencial.
- b. violar la política de seguridad del sistema. ✔
- c. hacerse con el control del sistema.
- d. hacer entrar al sistema en un modo de error.

La respuesta correcta es: violar la política de seguridad del sistema.

Pregunta **13**
Sin contestar
Puntúa como 1,00

Un administrador del servidor web configura ajustes de acceso para que los usuarios se autentiquen primero antes de acceder a determinados sitios web. ¿Qué requisito de seguridad informática se aborda en la configuración?

a. Disponibilidad
b. Integridad
c. Escalabilidad
d. Confidencialidad

La respuesta correcta es: Confidencialidad

Pregunta **14**
Correcta
Se puntúa 1,00 sobre 1,00

Las amenazas son posibles sucesos que pueden hacer que nuestro sistema funcione mal; existen a muchos niveles y en diversos modos que dependen de las malas intenciones de personas o colectivos, pero también de hechos completamente externos, por eso...

a. es preciso calcular la probabilidad de absolutamente todas las amenazas posibles.
b. es preciso calcular el riesgo de todas las amenazas posibles.
c. no podemos protegernos de absolutamente todas las amenazas posibles. ✔
d. es preciso prever absolutamente todas las amenazas posibles y poner contramedidas.

La respuesta correcta es: no podemos protegernos de absolutamente todas las amenazas posibles.

Pregunta **15**
Correcta
Se puntúa 1,00 sobre 1,00

En un sistema asimétrico de clave pública, si cifro un mensaje con mi clave privada, cualquier usuario puede descifrar (con mi clave pública).

a. Esto no proporciona integridad, pero proporciona confidencialidad, autenticidad del emisor y no repudio.
b. Esto no proporciona confidencialidad, pero proporciona integridad, autenticidad del emisor y no repudio. ✔
c. Esto no proporciona no repudio, pero proporciona integridad, autenticidad del emisor y confidencialidad.
d. Esto no proporciona autenticidad, pero proporciona integridad, confidencialidad y no repudio.

La respuesta correcta es: Esto no proporciona confidencialidad, pero proporciona integridad, autenticidad del emisor y no repudio.

Pregunta **16**
Correcta
Se puntúa 1,00 sobre 1,00

Si a un mensaje le aplicamos una función hash, ciframos el resultado con nuestra clave privada y se lo enviamos a un tercero junto con el mensaje original, conseguimos:

- a. Autenticación, Integridad y No repudio en origen ✔
- b. Autenticación, Confidencialidad y No repudio en origen
- c. Confidencialidad, Integridad y No repudio en origen
- d. Autenticación, Confidencialidad e Integridad

La respuesta correcta es: Autenticación, Integridad y No repudio en origen

Pregunta **17**
Correcta
Se puntúa 1,00 sobre 1,00

¿Cuál de las siguientes satisface una autenticación de usuario de dos factores

- a. Identificador de usuario más contraseña
- b. Escaneo de iris y de huella dactilar
- c. Identificador de usuario y sistema GPS
- d. Smartcard que requiere un código PIN ✔

La respuesta correcta es: Smartcard que requiere un código PIN

Pregunta **18**
Correcta
Se puntúa 1,00 sobre 1,00

Las amenazas más fácilmente detectables son

- a. Las de interrupción. ✔
- b. Las de interceptación.
- c. Las de modificación.
- d. Las de generación.

La respuesta correcta es: Las de interrupción.

Pregunta **19**

Correcta

Se puntúa 1,00 sobre 1,00

En un sistema asimétrico de clave pública, si cifro un mensaje con la clave pública del destino, sólo el destinatario podrá descifrarlo. Esto

a. proporciona autenticidad y confidencialidad, pero no proporciona integridad y no repudio.
b. proporciona autenticidad e integridad, pero no proporciona confidencialidad y no repudio.
c. proporciona confidencialidad e integridad; no proporciona autenticidad del emisor y no repudio. ✔
d. proporciona confidencialidad y no repudio, pero no proporciona integridad y autenticidad.

La respuesta correcta es: proporciona confidencialidad e integridad; no proporciona autenticidad del emisor y no repudio.

Pregunta **20**

Correcta

Se puntúa 1,00 sobre 1,00

Una empresa experimenta muchísimas visitas en un servidor web principal. El departamento de TI está desarrollando un plan para agregar un par más de servidores web para equilibrar la carga y la redundancia. ¿Qué requisito de seguridad informática se aborda en la implementación del plan?

a. Escalabilidad
b. Disponibilidad ✔
c. Confidencialidad
d. Integridad

La respuesta correcta es: Disponibilidad

Pregunta **21**

Correcta

Se puntúa 1,00 sobre 1,00

En relación a la firma digital, el servicio de "No repudio" :

a. Garantiza que los datos recibidos han sido enviados por una entidad autorizada.
b. Previene del uso no autorizado de un recurso.
c. Protege contra la negación de autoría frente a terceras partes. ✔
d. Protege contra el acceso no autorizado a la información.

La respuesta correcta es: Protege contra la negación de autoría frente a terceras partes.

Pregunta **22**

Correcta

Se puntúa 1,00 sobre 1,00

Tras ejecutar dos interlocutores el algoritmo de Diffie-Hellman

a. Uno ha cifrado un mensaje para el otro con criptografía simétrica y el otro lo ha descifrado

b. Ambos han convenido una clave simétrica a través de un canal público ✔

c. Ambos han convenido una clave asimétrica a través de un canal público

d. Uno ha cifrado un mensaje para el otro con criptografía asimétrica y el otro lo ha descifrado

La respuesta correcta es: Ambos han convenido una clave simétrica a través de un canal público

Pregunta **23**

Correcta

Se puntúa 1,00 sobre 1,00

En un criptosistema compuesto por n usuarios:

a. Si se utiliza cifrado simétrico el número total de claves implicadas es 2n.

b. Si se utiliza cifrado asimétrico el número total de claves implicadas es 2n. ✔

c. Si se utiliza cifrado asimétrico el número de claves que maneja un usuario es 2n.

d. Si se utiliza cifrado simétrico el número de claves que maneja un usuario es 2n.

La respuesta correcta es: Si se utiliza cifrado asimétrico el número total de claves implicadas es 2n.

Pregunta **24**

Sin contestar

Puntúa como 1,00

En los modos de cifrado de bloque:

a. En el modo ECB, cada bloque cifrado depende del bloque cifrado anteriormente.

b. En todos los modos de cifrado de bloque, cada bloque se cifra separadamente de los demás sin dependencia de otros bloques.

c. En el modo CFB, un error en un bit del criptograma afectará sólo a un bloque del texto en claro recuperado.

d. En el modo CBC, el texto cifrado correspondiente a un determinado bloque de texto en claro depende del bloque de texto cifrado anterior. Asimismo, el bloque de texto en claro correspondiente a un determinado bloque de texto cifrado depende del bloque de texto cifrado anterior.

La respuesta correcta es: En el modo CBC, el texto cifrado correspondiente a un determinado bloque de texto en claro depende del bloque de texto cifrado anterior. Asimismo, el bloque de texto en claro correspondiente a un determinado bloque de texto cifrado depende del bloque de texto cifrado anterior.

Pregunta **25**

Correcta

Se puntúa 1,00 sobre 1,00

La principal vulnerabilidad de las funciones hash son los ataques basados en:

- a. La fuerza bruta.
- b. El cifrado cíclico.
- c. Los bits de relleno por bloques.
- d. La paradoja del cumpleaños. ✔

La respuesta correcta es: La paradoja del cumpleaños.

Pregunta **26**

Correcta

Se puntúa 1,00 sobre 1,00

Un certificado digital

- a. Contiene datos identificativos de una persona validados de forma electrónica. ✔
- b. Contiene el hash de la clave privada de la persona.
- c. Es un documento en formato analógico que contiene datos de una persona.
- d. Se diferencia de la firma electrónica en que solo sirve para validar la firma manuscrita.

La respuesta correcta es: Contiene datos identificativos de una persona validados de forma electrónica.

Pregunta **27**

Sin contestar

Puntúa como 1,00

Las comunicaciones no cifradas son...

- a. un riesgo.
- b. una vulnerabilidad.
- c. un ataque.
- d. una amenaza.

La respuesta correcta es: una vulnerabilidad.

Pregunta **28**
Correcta
Se puntúa 1,00 sobre 1,00

En el cifrado en flujo One-Time Pad, la longitud de la clave de cifrado es...

- a. Igual a la del mensaje. ✔
- b. Menor que la del mensaje.
- c. Mayor que la del mensaje.
- d. De 64 bits.

La respuesta correcta es: Igual a la del mensaje.

Pregunta **29**
Sin contestar
Puntúa como 1,00

Se define como "La propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad " a la

- a. Trazabilidad
- b. Confidencialidad
- c. Integridad
- d. Autenticidad

La respuesta correcta es: Trazabilidad

Pregunta **30**
Correcta
Se puntúa 1,00 sobre 1,00

Es cierto que

- a. La vulnerabilidad genera un riesgo, que la amenaza puede aprovechar para realizar el ataque en un sistema informático.
- b. El riesgo es la posibilidad de que una amenaza se produzca aprovechando una vulnerabilidad, dando lugar a un ataque al equipo.
- c. Las tres anteriores son diferentes formas de expresar la misma idea. ✔
- d. Un riesgo es la probabilidad de que se produzca una amenaza, dando lugar a un ataque que explota una vulnerabilidad del sistema.

La respuesta correcta es: Las tres anteriores son diferentes formas de expresar la misma idea.

Pregunta **31**

Correcta

Se puntúa 1,00 sobre 1,00

¿Qué tipo de ingeniería social es la que suplanta la apariencia o nombre de la entidad afectada?

- a. Phishing ✔
- b. Keyloggers
- c. Pharming
- d. Spam

La respuesta correcta es: Phishing

Pregunta **32**

Sin contestar

Puntúa como 1,00

Una vulnerabilidad crítica:

- a. Se puede reducir en gran medida a partir de configuraciones predeterminadas.
- b. Puede poner en peligro la integridad o disponibilidad de los recursos de procesamiento.
- c. Se produce cuando el sistema está en un momento crítico.
- d. Puede permitir la propagación de un gusano de internet sin la acción del usuario.

La respuesta correcta es: Puede poner en peligro la integridad o disponibilidad de los recursos de procesamiento.

Pregunta **33**

Sin contestar

Puntúa como 1,00

Imagina un sencillo sistema informático que simula un ciclista, al que le pueden pasar cosas tan inesperadas como [a] "caerse de la bici" o [b] "ser embestido por un peatón". En este caso, ¿qué es cada uno de estos dos sucesos?

- a. [a] es una vulnerabilidad, y [b] un posible riesgo.
- b. [a] es un posible riesgo, y [b] una amenaza.
- c. tanto [a] como [b] son posibles riesgos medibles.
- d. [a] es una amenaza, y [b] una vulnerabilidad.

La respuesta correcta es: [a] es un posible riesgo, y [b] una amenaza.

Pregunta **34**

Sin contestar

Puntúa como 1,00

SHA-1 produce un valor hash de:

a. 33 bytes
b. 256 bits
c. 20 bytes
d. 256 y 512 bits, respectivamente

La respuesta correcta es: 256 bits

Pregunta **35**

Incorrecta

Se puntúa -0,33 sobre 1,00

En una comunicación, ¿hay una forma habitual de utilizar algoritmos simétricos y asimétricos, conjuntamente?

a. Sí. El asimétrico para cifrar y el simétrico para intercambiar las claves públicas y privadas. ✖
b. Sí. El simétrico para cifrar y el asimétrico para intercambiar la clave.
c. Nunca. Son incompatibles.
d. Sí, siempre que la clave sea un número primo "grande".

La respuesta correcta es: Sí. El simétrico para cifrar y el asimétrico para intercambiar la clave.

Pregunta **36**

Correcta

Se puntúa 1,00 sobre 1,00

Una función hash segura debe tener la siguiente característica:

a. Ser resistente a ataques por estadísticas del lenguaje.
b. Ser resistente a colisiones. ✔
c. Poseer una clave de al menos 128 bits.
d. Realizar todos los cálculos con palabras de 32 bits.

La respuesta correcta es: Ser resistente a colisiones.

Pregunta **37**

Correcta

Se puntúa 1,00 sobre 1,00

El robo de información de identificación personal, como información de tarjetas de crédito es un ejemplo de qué tipo de ataque sobre la

- a. Confidencialidad ✔
- b. Autenticidad
- c. Integridad
- d. Disponibilidad

La respuesta correcta es: Confidencialidad

Pregunta **38**

Correcta

Se puntúa 1,00 sobre 1,00

Existen cuatro tipos de amenazas a los assets del sistema que provienen de vulnerabilidades del sistema. Son generación, interceptación...

- a. modificación e interrupción. ✔
- b. interrupción y degradación.
- c. denegación e interrupción.
- d. integridad y confidencialidad.

La respuesta correcta es: modificación e interrupción.

Pregunta **39**

Sin contestar

Puntúa como 1,00

Una pérdida de datos, se cataloga entre las amenazas posibles de un sistema como un ataque...

- a. por generación, de datos.
- b. por modificación, de datos.
- c. por interrupción, de datos.
- d. por interceptación, de software.

La respuesta correcta es: por interrupción, de datos.

Pregunta **40**
Correcta
Se puntúa 1,00 sobre 1,00

Al aplicar el principio de diseño de sistemas seguros enunciado por Saltzer y Schoeder denominado "del menor privilegio posible", ayudamos a minimizar las consecuencias negativas de los errores, pero además...

- a. reducimos los efectos negativos de los ataques desde el interior. ✔
- b. reducimos los efectos negativos de los ataques desde el exterior.
- c. maximizamos la ventana de oportunidad del adversario.
- d. podemos concentrar las medidas de seguridad en compartimentos específicos.

La respuesta correcta es: reducimos los efectos negativos de los ataques desde el interior.

Pregunta **41**
Sin contestar
Puntúa como 1,00

¿Cuál de las siguientes situaciones NO puede considerarse un incidente?

- a. Un evento cuyo impacto no genere una interrupción prolongada del servicio
- b. Un uso no autorizado de la cuenta de un usuario
- c. Fallo hardware
- d. Todas las situaciones anteriores se considerarían incidentes

La respuesta correcta es: Todas las situaciones anteriores se considerarían incidentes

Pregunta **42**
Correcta
Se puntúa 1,00 sobre 1,00

El principio de Kerckhoff dice: "Todos los algoritmos deben ser públicos; sólo las claves deben ser secretas". Al diseñar un sistema que obedece a este principio nos encuadramos en el fundamento de seguridad de...

- a. exposición mínima.
- b. abrir el diseño. ✔
- c. simplificación.
- d. mediación completa.

La respuesta correcta es: abrir el diseño.

Pregunta **43**

Sin contestar

Puntúa como 1,00

¿Durante qué proceso de la gestión de los riesgos se determina que se va a hacer una transferencia del riesgo?

- a. Planificar la respuesta a los riesgos
- b. Realizar el análisis cuantitativo de riesgos
- c. Monitorear y controlar los riesgos
- d. Identificar los riesgos

La respuesta correcta es: Planificar la respuesta a los riesgos

Pregunta **44**

Correcta

Se puntúa 1,00 sobre 1,00

Desde una perspectiva generalista, agrupamos las medidas de seguridad en tres grandes bloques...

- a. Defensa, confidencialidad e integridad.
- b. Defensa, disuasión y detección. ✔
- c. Dependibilidad, seguridad y robustez.
- d. Defensa, disponibilidad y dependibilidad.

La respuesta correcta es: Defensa, disuasión y detección.

Pregunta **45**

Correcta

Se puntúa 1,00 sobre 1,00

Según la metodología MAGERIT, el riesgo remanente en el sistema tras la implantación de las salvaguardas determinadas en el plan de seguridad de la información se denomina

- a. Riesgo acumulado
- b. Riesgo residual ✔
- c. Riesgo retenido
- d. Riesgo supervisado

La respuesta correcta es: Riesgo residual

Pregunta **46**

Correcta

Se puntúa 1,00 sobre 1,00

La definición de servicios básicos de seguridad indicada en la norma ISO 7498 (también conocida como ITU X.800) se centra en el entorno de las comunicaciones y especifica como servicios básicos...

a. No Repudio, Control de Acceso, Contabilidad, Confidencialidad y Autenticación.
b. Integridad de Datos, Contabilidad, Confidencialidad, No Repudio y Control de Acceso.
c. Autorización, Autenticación, No Repudio, Confidencialidad y Control de Acceso.
d. Autenticación, Integridad de Datos, No Repudio, Confidencialidad y Control de Acceso. ✔

La respuesta correcta es: Autenticación, Integridad de Datos, No Repudio, Confidencialidad y Control de Acceso.

Pregunta **47**

Sin contestar

Puntúa como 1,00

En criptografía asimétrica:

a. El algoritmo de clave pública de Diffie-Hellman permite el acuerdo entre dos entidades de una clave simétrica, a través de comunicaciones exclusivamente públicas.
b. Todas las anteriores son correctas.
c. El criptoanálisis del algoritmo de Diffie-Hellman se basa en la resolución del problema del logaritmo discreto.
d. El algoritmo de cifrado de ElGamal, produce bloques de texto cifrado mayores que los bloques de texto en claro.

La respuesta correcta es: Todas las anteriores son correctas.

Pregunta **48**

Correcta

Se puntúa 1,00 sobre 1,00

Alice y Bob utilizan una firma digital para firmar un documento. ¿Qué clave debe utilizar Alice para firmar el documento de modo que Bob pueda asegurarse de que el documento proviene de Alice?

a. clave privada de Bob
b. clave pública de Alice
c. nombre de usuario y contraseña de Alice
d. clave privada de Alice ✔

La respuesta correcta es: clave privada de Alice

Pregunta **49**

Correcta

Se puntúa 1,00 sobre 1,00

Señale la respuesta correcta. En una comunicación HTTPS, ¿qué tipo de cifrado se utiliza?

a. Asimétrico exclusivamente

b. Tanto el simétrico como el asimétrico ✔

c. Simétrico exclusivamente

d. No se utiliza ningún cifrado

La respuesta correcta es: Tanto el simétrico como el asimétrico

Pregunta **50**

Correcta

Se puntúa 1,00 sobre 1,00

La medida del daño producido por un incidente de seguridad se denomina

a. Vulnerabilidad

b. Impacto ✔

c. Riesgo

d. Amenaza

La respuesta correcta es: Impacto