Comenzado el	viernes, 29 de septiembre de 2023, 14:44
Estado	Finalizado
Finalizado en	viernes, 29 de septiembre de 2023, 15:59
Tiempo empleado	1 hora 14 minutos
Calificación	**116,00** de 116,00 (**100**%)

Pregunta **1**

Correcta

Se puntúa 5,00 sobre 5,00

¿Qué control de los siguientes asegura la integridad?

Seleccione una:

- a. Encriptación simétrica
- b. Encriptación asimétrica
- c. Algoritmo de hash (ej. SHA2) ✔
- d. Autentificación
- e. AES

Respuesta correcta

La respuesta correcta es: Algoritmo de hash (ej. SHA2)

Pregunta **2**

Correcta

Se puntúa 6,00 sobre 6,00

Usted se encuentra desarrollando el sistema web una aplicación para e-commerce. Usted al revisar las buenas prácticas de seguridad, advierte que es necesario incorporar los siguientes requerimientos.

Indique que propiedad se quiere lograr con dichas funcionalidades.

Una funcionalidad que me permita identificar si una transacción crítica fue modificada.	Integridad ✔
Una funcionalidad que corrobore que el usuario realizó una compra.	No repudio ✔
Una funcionalidad de notificación cuando alguna acción en el sistema no se complete correctamente.	Disponibilidad ✔
Una funcionalidad que me permita visualizar las acciones del usuario en el sistema.	Accountability ✔
Una funcionalidad que me permita saber que la persona que ingreso a la web es quien dice ser.	Autenticidad ✔
Una funcionalidad para que solamente el jefe de finanzas de la cuenta pueda ver datos privados del cliente.	Confidencialidad ✔

Respuesta correcta

La respuesta correcta es: Una funcionalidad que me permita identificar si una transacción crítica fue modificada. → Integridad, Una funcionalidad que corrobore que el usuario realizó una compra. → No repudio, Una funcionalidad de notificación cuando alguna acción en el sistema no se complete correctamente. → Disponibilidad,
Una funcionalidad que me permita visualizar las acciones del usuario en el sistema. → Accountability, Una funcionalidad que me permita saber que la persona que ingreso a la web es quien dice ser. → Autenticidad, Una funcionalidad para que solamente el jefe de finanzas de la cuenta pueda ver datos privados del cliente. → Confidencialidad

Pregunta **3**

Correcta

Se puntúa 6,00 sobre 6,00

Relacione el objetivo de ciberseguridad con su definición correspondiente.

La propiedad de que los datos no se divulgan a las entidades del sistema a menos que hayan sido autorizados para conocer los datos. → Confidencialidad

La propiedad de ser genuino y poder ser verificado y confiable. Esto significa verificar que los usuarios son quienes dicen ser y que cada entrada que llega al sistema proviene de una fuente confiable. → Autenticidad (Authenticity)

La propiedad de que los datos no se han cambiado, destruido o perdido de manera no autorizada o accidental. → Integridad (Integrity)

La propiedad de un sistema o un recurso del sistema que es accesible o utilizable u operacional bajo demanda, por una entidad autorizada del sistema, de acuerdo con las especificaciones de rendimiento del sistema; es decir, un sistema está disponible si proporciona servicios de acuerdo con el diseño del sistema cuando los usuarios lo soliciten. → Disponibilidad (Availability)

Garantía de que el remitente de la información es provisto con una prueba de entrega y el destinatario recibe la prueba de la identidad del remitente, por lo que ninguno de los dos puede negar más tarde haber procesado la información. → No repudio

La propiedad de un sistema o recurso del sistema que garantiza que las acciones de una entidad del sistema puedan rastrearse de forma exclusiva a esa entidad, que luego puede ser considerada responsable de sus acciones. → Rendición de cuentas (Accountability)

Respuesta correcta

La respuesta correcta es:
La propiedad de que los datos no se divulgan a las entidades del sistema a menos que hayan sido autorizados para conocer los datos. → Confidencialidad, La propiedad de ser genuino y poder ser verificado y confiable. Esto significa verificar que los usuarios son quienes dicen ser y que cada entrada que llega al sistema proviene de una fuente confiable. → Autenticidad (Authenticity),
La propiedad de que los datos no se han cambiado, destruido o perdido de manera no autorizada o accidental. → Integridad (Integrity),
La propiedad de un sistema o un recurso del sistema que es accesible o utilizable u operacional bajo demanda, por una entidad autorizada del sistema, de acuerdo con las especificaciones de rendimiento del sistema; es decir, un sistema está disponible si proporciona servicios de acuerdo con el diseño del sistema cuando los usuarios lo soliciten. → Disponibilidad (Availability), Garantía de que el remitente de la información es provisto con una prueba de entrega y el destinatario recibe la prueba de la identidad del remitente, por lo que ninguno de los dos puede negar más tarde haber procesado la información. → No repudio, La propiedad de un sistema o recurso del sistema que garantiza que las acciones de una entidad del sistema puedan rastrearse de forma exclusiva a esa entidad, que luego puede ser considerada responsable de sus acciones. → Rendición de cuentas (Accountability)

Pregunta **4**

Correcta

Se puntúa 10,00 sobre 10,00

Relacione los conceptos con su definición o ejemplo dado.

Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron.	No repudio
Conservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio	Ciberprotección
En un documento electrónico, puedo obtener la presente propiedad a través de la utilización de técnicas de encriptación asimétrica y simétrica (ej. RSA y AES)	Confidencialidad
Si instalo aplicaciones de terceros en mi smartphone, sin preocuparme por su origen, es probable que tenga una...	Vulnerabilidad
Cuando necesito iniciar sesión en un sitio web y este me solicita mi clave de ingreso y un código enviado a mi celular. En este caso, el banco esta verificando mi...	Autenticidad
Ej. Un Datacenter TIER IV tiene un 99.995% de .... lo que equivale a que puede que este se encuentre sin servicio durante 26 minutos al año. Este tipo de Datacenter poseen altas exigencias. Por ejemplo de redundancia, escalabilidad, enfriamiento, entre otros factores.	Disponibilidad
Peligro de inundación	Amenaza
El proceso de proteger la información mediante la prevención, detección y respuesta a los ataques	Ciberseguridad
Intenciones y dirección de una organización, como las expresa formalmente su alta dirección	Política
Firewall que permite conexiones desde el exterior a puertos no comunes en conjunto a un software malicioso que se hace pasar por el original. Este crea conexiones a una estación de control externa a la organización.	Vector de ataque

La respuesta correcta es: Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto suceso o se realizó una cierta acción por parte de las entidades que lo originaron. → No repudio, Conservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio → Ciberprotección, En un documento electrónico, puedo obtener la presente propiedad a través de la utilización de técnicas de encriptación asimétrica y simétrica (ej. RSA y AES) → Confidencialidad, Si instalo aplicaciones de terceros en mi smartphone, sin preocuparme por su origen, es probable que tenga una... → Vulnerabilidad, Cuando necesito iniciar sesión en un sitio web y este me solicita mi clave de ingreso y un código enviado a mi celular. En este caso, el banco esta verificando mi... → Autenticidad, Ej. Un Datacenter TIER IV tiene un 99.995% de ....
lo que equivale a que puede que este se encuentre sin servicio durante 26 minutos al año.
Este tipo de Datacenter poseen altas exigencias. Por ejemplo de redundancia, escalabilidad, enfriamiento, entre otros factores. → Disponibilidad, Peligro de inundación → Amenaza, El proceso de proteger la información mediante la prevención, detección y respuesta a los ataques → Ciberseguridad, Intenciones y dirección de una organización, como las expresa formalmente su alta dirección → Política, Firewall que permite conexiones desde el exterior a puertos no comunes en conjunto a un software malicioso que se hace pasar por el original. Este crea conexiones a una estación de control externa a la organización. → Vector de ataque

Pregunta **5**

Correcta

Se puntúa 5,00 sobre 5,00

Una organización busca asegurar que un empleado autorizado pueda acceder a sus recursos durante las horas normales de operación del negocio. ¿Que concepto de seguridad se encuentra involucrado?

Seleccione una:

- a. Disponibilidad ✔
- b. Confidencialidad
- c. No repudio
- d. Rendición de cuentas
- e. Integridad

Respuesta correcta

La respuesta correcta es: Disponibilidad

Pregunta **6**

Correcta

Se puntúa 9,00 sobre 9,00

Indique el concepto de acuerdo a la definición entregada.

Camino o medios por los cuales un atacante puede obtener acceso a un servidor de computador o de red para entregar un resultado malicioso.	Vector de ataque
Persona o grupo de personas en la(s) que los órganos de gobierno han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la organización.	Dirección ejecutiva
Riesgo remanente después del tratamiento del riesgo.	Riesgo residual
Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad	Control de acceso
Declaración que describe lo que quiere lograr como resultado de la implementación de controles.	Objetivo de control
Intenciones y dirección de una organización, como las expresa formalmente su alta dirección.	Política
Persona o grupo de personas que dirigen y controlan una organización al más alto nivel.	Alta dirección
Evento singular o serie de eventos, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.	Incidente de seguridad de la información
Software de control remoto, específicamente una colección de bots maliciosos, que corre de manera autónoma y automática en computadores comprometidos.	Botnet

Respuesta correcta

La respuesta correcta es:
Camino o medios por los cuales un atacante puede obtener acceso a un servidor de computador o de red para entregar un resultado malicioso.
→ Vector de ataque, Persona o grupo de personas en la(s) que los órganos de gobierno han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la organización. → Dirección ejecutiva, Riesgo remanente después del tratamiento del riesgo. → Riesgo residual, Medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de negocio y de seguridad → Control de acceso, Declaración que describe lo que quiere lograr como resultado de la implementación de controles. → Objetivo de control, Intenciones y dirección de una organización, como las expresa formalmente su alta dirección. → Política, Persona o grupo de personas que dirigen y controlan una organización al más alto nivel. → Alta dirección, Evento singular o serie de eventos, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información. → Incidente de seguridad de la información, Software de control remoto, específicamente una colección de bots maliciosos, que corre de manera autónoma y automática en computadores comprometidos. → Botnet

Pregunta **7**

Correcta

Se puntúa 5,00 sobre 5,00

Un control se gestiona para mitigar el riesgo inherente.

Seleccione una:

- Verdadero ✔
- Falso

El riesgo residual se gestiona mitigando, aceptando, transfiriendo o evitando.

El control se utiliza solamente en caso de que se quiera mitigar el riesgo inherente.

La respuesta correcta es 'Verdadero'

Pregunta **8**

Correcta

Se puntúa 5,00 sobre 5,00

¿Como afecta el ransomware a la triada de la seguridad de la información?

- Confidencialidad ✔ : Amenaza la filtración de datos hacia internet para asegurar el pago del rescate.
- Integridad ✔ : Modificación y alteración de la información, por lo que ahora se encuentra alterada.
- Disponibilidad ✔ : Datos cifrados, no se puede acceder.

Respuesta correcta

La respuesta correcta es:
¿Como afecta el ransomware a la triada de la seguridad de la información?

- [Confidencialidad]: Amenaza la filtración de datos hacia internet para asegurar el pago del rescate.
- [Integridad]: Modificación y alteración de la información, por lo que ahora se encuentra alterada.
- [Disponibilidad]: Datos cifrados, no se puede acceder.

Pregunta **9**

Correcta

Se puntúa 5,00 sobre 5,00

Una APT (Advanced Persistent Threat) se refiere a un de ciberataque altamente sofisticado y preciso desde múltiples frentes, ejecutado por grupos que a menudo son apoyados o financiados por entidades externos, cuyas principales características son:

- Acuciosidad en la seguridad de sus operaciones.
- Bajas tasas de detección.
- Altas probabilidades de éxito en el cumplimiento de sus objetivos.

Seleccione una:

- Verdadero ✔
- Falso

La respuesta correcta es 'Verdadero'

Pregunta **10**

Correcta

Se puntúa 5,00 sobre 5,00

Entre los desafíos de la seguridad tenemos los siguientes:

i. El cambio constante en la tecnología supone una actualización continua de las medidas de seguridad.

ii. La gran cantidad de dispositivos de diferentes y cada uno de ellos con la necesidad de requerir acceso a recursos es enorme. Esto se debe controlar con medidas de seguridad.

iii. Las amenazas vienen desde pocos actores y estas son constantes en el tiempo.

iv. El usuario requiere de la habilitación de nuevas funcionalidades y tecnologías cada vez más potentes, lo cual debe ser acompañado por una seguridad robusta.

v. Los costos de la seguridad en general son muy elevados, sin embargo los beneficios por lo general son difíciles de calcular.

Seleccione una:

- a. i, ii, iii, iv y v
- b. i y ii
- c. i, ii, iv y v ✔
- d. i, ii, iv, y v
- e. i, ii, iii

Respuesta correcta

Las respuestas correctas son: i, ii, iv, y v, i, ii, iv y v

Pregunta **11**

Correcta

Se puntúa 5,00 sobre 5,00

Los usuarios quieren tecnología con las características más modernas y potentes, que sea conveniente de usar, que ofrezca el anonimato en ciertas circunstancias y que sea segura. Pero existe un conflicto inherente entre una mayor facilidad de uso y una mayor gama de opciones por un lado, y una seguridad robusta por el otro. De acuerdo a lo anterior, indique cuales de las siguientes afirmaciones es verdadera:

i) En general, cuanto más simple es el sistema y cuanto más aislados están sus elementos individuales, más fácil es implementar una seguridad efectiva.

ii) A mayor complejidad que resulta hace que los sistemas sean menos seguros.

iii) Los usuarios o grupos dentro de una organización que se sientan incómodos por los mecanismos de seguridad se verán tentados a encontrar formas de evitar esos mecanismos.

iv) La funcionalidad de los sistemas debe ir de la mano con la seguridad. No se debe poner una sobre la otra.

v) Los usuarios podrían exigir la relajación de los requisitos de seguridad en caso de que esta obstaculice su trabajo.

Seleccione una:

- a. i y iii
- b. Todas las afirmaciones son falsas
- c. Todas las afirmaciones son verdaderas ✔
- d. i, ii, iii y v
- e. i, ii y iii

Respuesta correcta

La respuesta correcta es: Todas las afirmaciones son verdaderas

Pregunta **12**

Correcta

Se puntúa 5,00 sobre 5,00

De las siguientes definiciones, cual(es) corresponde a la de Ciberseguridad:

i. Estado de estar protegido en el Ciberespacio contra de consecuencias sociales, psicológicas, financieras, emocionales, ocupacionales, espirituales, físicas, educacionales o de otro tipo que resultan del daño, fallo, error, accidentes, menoscabo o cualquier otro suceso que se pueda considerar no deseable.

ii. El proceso de proteger la información mediante la prevención, detección y respuesta los ataques.

iii. Protección de todos los activos físicos de la organización.

iv. Preservación de la confidencialidad de los datos digitales.

v. Es un conjunto de políticas, conceptos, medidas, mejores prácticas, aseguramiento, enfoques de gestión de riesgos, pautas, herramientas y tecnologías que se utilizan para proteger el entorno y la organización del ciberespacio y los activos de los usuarios.

Seleccione una:

- a. i, ii y iii
- b. i, ii y v ✔
- c. ii, iii, iv y v
- d. i, ii, iii y iv
- e. i, iii y v

La iii y iv corresponden a definiciones mas cercanas a la seguridad de la información.

La respuesta correcta es: i, ii y v

Pregunta **13**

Correcta

Se puntúa 5,00 sobre 5,00

En las noticias de diferentes sitios de seguridad, apareció una nota sobre la amenaza ✔ que corresponde a inyección de código en un plugin muy popular del gestor de contenidos Wordpress. En esta se recomienda, como buena práctica revisar si mi empresa tiene algún nivel de exposición ✔ , revisando mis sistemas web.

Luego de comprobar mis sistemas, me dí cuenta que en un par de sitios de la empresa tengo la versión 1.3 del plugin, justamente la que tiene la vulnerabilidad ✔ . Por lo tanto, aplico los controles ✔ necesarios para disminuir el riesgo ✔ .

Respuesta correcta

La respuesta correcta es:

En las noticias de diferentes sitios de seguridad, apareció una nota sobre la [amenaza] que corresponde a inyección de código en un plugin muy popular del gestor de contenidos Wordpress. En esta se recomienda, como buena práctica revisar si mi empresa tiene algún nivel de [exposición], revisando mis sistemas web.

Luego de comprobar mis sistemas, me dí cuenta que en un par de sitios de la empresa tengo la versión 1.3 del plugin, justamente la que tiene la [vulnerabilidad] . Por lo tanto, aplico los [controles] necesarios para disminuir el [riesgo].

Pregunta **14**

Correcta

Se puntúa 9,00 sobre 9,00

Un atacante ✔ , debe sortear varios tipos de controles ✔ antes de ganar acceso a los activos críticos ✔ de la organización.

Una buena estrategia para el defensor ✔ , es adoptar una defensa en profundidad ✔ . Para ello, lo se debe establecer una aproximación en capas ✔ . Para ello, se debe coordinar y usar varios mecanismos de protección. Este esquema permite mitigar ✔ la probabilidad de compromiso y penetraciones exitosas ✔ . El número de capas, depende de la sensibilidad del activo ✔ .

Respuesta correcta

La respuesta correcta es:
Un [atacante], debe sortear varios tipos de [controles] antes de ganar acceso a los [activos críticos] de la organización.

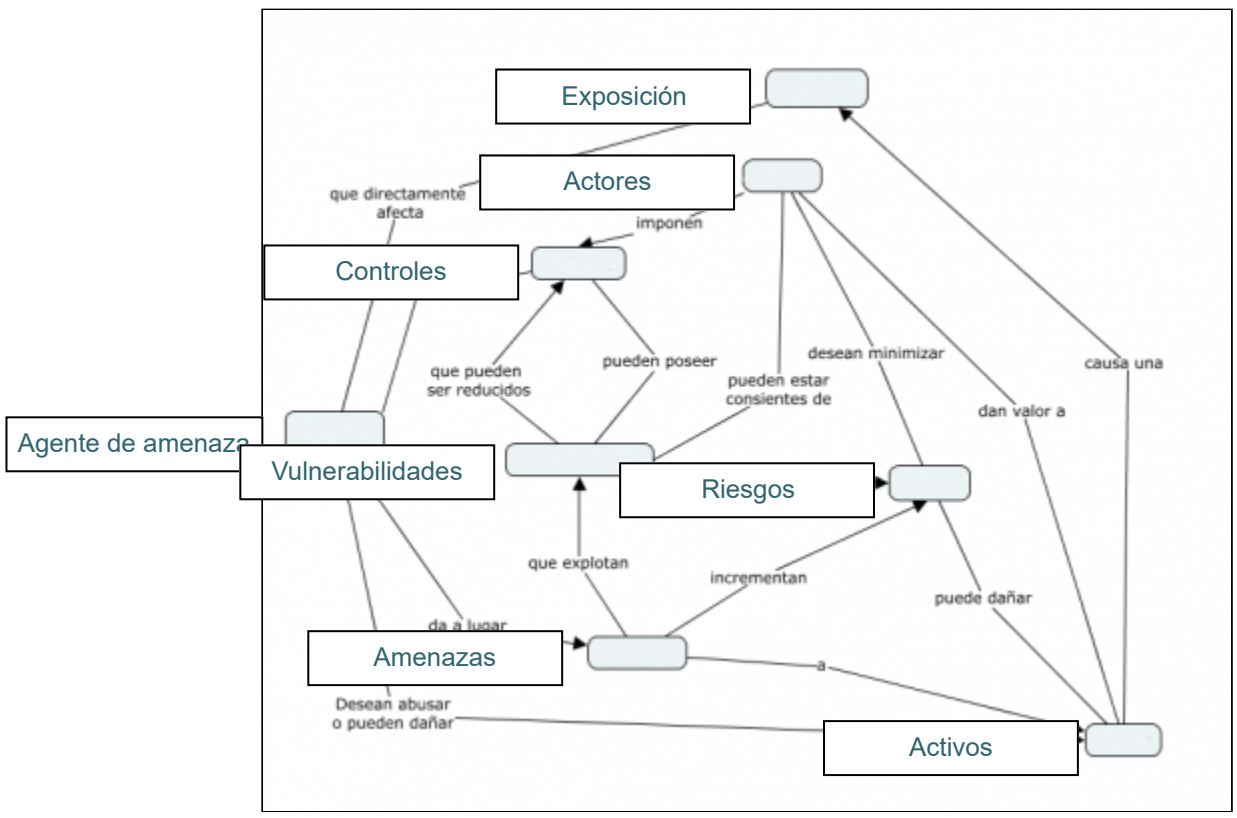
Una buena estrategia para el [defensor], es adoptar una [defensa en profundidad]. Para ello, lo se debe establecer una [aproximación en capas]. Para ello, se debe coordinar y usar varios mecanismos de protección. Este esquema permite [mitigar] la probabilidad de [compromiso y penetraciones exitosas]. El número de capas, depende de la [sensibilidad del activo].

Pregunta **15**

Correcta

Se puntúa 8,00 sobre 8,00

Arrastra el concepto donde corresponda.



Respuesta correcta

Pregunta **16**

Correcta

Se puntúa 5,00 sobre 5,00

Asocie cada concepto con un ejemplo del mismo

Comprobación hash, luego de descargado un archivo, para ver si este corresponde con el publicado en su pagina web origen.	Integridad ✔
Envío de datos encriptado desde el navegador a un servidor HTTPS	Confidencialidad ✔
Un servidor HTTP que tiene abiertos otros servicios como SSH y FTP.	Vulnerabilidad ✔
Varios servidores HTTP, con el mismo contenido, distribuyendo la carga de las consultas que llegan desde Internet.	Disponibilidad ✔
Error no intencional al ingresar datos en un formulario web.	Amenaza ✔

Respuesta correcta

La respuesta correcta es: Comprobación hash, luego de descargado un archivo, para ver si este corresponde con el publicado en su pagina web origen. → Integridad, Envío de datos encriptado desde el navegador a un servidor HTTPS → Confidencialidad, Un servidor HTTP que tiene abiertos otros servicios como SSH y FTP. → Vulnerabilidad, Varios servidores HTTP, con el mismo contenido, distribuyendo la carga de las consultas que llegan desde Internet. → Disponibilidad, Error no intencional al ingresar datos en un formulario web. → Amenaza

Pregunta **17**

Correcta

Se puntúa 5,00 sobre 5,00

Es difícil estimar el costo total de las infracciones de ciberseguridad y, por lo tanto, los beneficios de las políticas y mecanismos de seguridad.

Seleccione una:

- (•) Verdadero ✔
- ( ) Falso

Dificultad para estimar costos y beneficios: es difícil estimar el costo total de las infracciones de ciberseguridad y, por lo tanto, los beneficios de las políticas y mecanismos de seguridad. Esto complica la necesidad de lograr un consenso sobre la asignación de recursos a la seguridad.

La respuesta correcta es 'Verdadero'

Pregunta **18**

Correcta

Se puntúa 5,00 sobre 5,00

Los activos de la organización en el ciberespacio están bajo amenaza constante por los siguientes agentes:

i. Vándalos y delincuentes

ii. Terroristas,

iii. Estados hostiles y otros actores maliciosos.

iv. Empresas

v. Gobiernos

¿Cuales de los anteriores corresponden a agentes de amenazas?

Seleccione una:

- a. Todos los indicados corresponden a agentes de amenazas. ✔
- b. i, ii y iii
- c. i, ii, iii y iv
- d. Ninguna de las otras opciones es correcta
- e. iv y v

Respuesta correcta

Naturaleza de la amenaza: los activos de la organización en el ciberespacio están bajo amenaza constante y en evolución desde vándalos, delincuentes, terroristas, estados hostiles y otros actores maliciosos. Además, una variedad de actores legítimos, incluidas las empresas y los gobiernos, están interesados en recopilar, analizar y almacenar información de y sobre individuos y organizaciones, lo que puede crear riesgos de seguridad y privacidad.

La respuesta correcta es: Todos los indicados corresponden a agentes de amenazas.

Pregunta **19**

Correcta

Se puntúa 3,00 sobre 3,00

Una amenaza es un motivo posible de un incidente indeseado, que puede implicar un menoscabo en una organización.

Seleccione una:

- Verdadero ✔
- Falso

La definición se refiere a amenaza

La respuesta correcta es 'Verdadero'

Pregunta **20**

Correcta

Se puntúa 5,00 sobre 5,00

La ingeniería social es la técnica en la que se utilizan las redes sociales para obtener información de una víctima.

Seleccione una:

- Verdadero
- Falso ✔

La Ingeniería Social, es y seguirá siendo la técnica más eficiente y menos costosa para las ciberoperaciones delictuales, debido al bajo riesgo para los atacantes y su particularidad de estar orientada a la manipulación inteligente de la tendencia natural de la gente a confiar valiéndose así de las personas y no del sistema operativo o equipamiento de seguridad.

No podemos olvidar que el usuario es el eslabón más importante de la cadena de la seguridad, por lo que su acción o inacción serán fundamentales a la hora de corregir vulnerabilidades, protegerse ante ciberataques o evitar caer en las trampas de los ciberdelincuentes.

La respuesta correcta es 'Falso'

◄ NOTAS PARCIALES

Ir a...

1.1. INTRODUCCIÓN ►