1. El impacto de una vulnerabilidad es ... (sólo una correcta)

a. La diferencia entre la probabilidad de ṕerdida de los objetos de valor antes y después de que se

explote la vulnerabilidad.

b. La diferencia entre los valores asociados al estado de los objetos de valor antes y después de que

se explote la vulnerabilidad.

c. La frecuencia con que se puede sacar partido de la vulnerabilidad.

d. El producto entre los valores asociados al estado de los objetos de valor antes y después de que se

explote la vulnerabilidad.

2. En Gestión de la Seguridad, la justificación de los controles de seguridad y la ponderación de sus beneficios frente a los costes que conlleve su implantación constituye el objetivo esencial de…

a. El análisis de riesgos.

b. La planificación.

c. Los controles físicos.

d. Las políticas de seguridad.

3. Para comprobar desde su ordenador, que tiene instalado Linux, si el equipo 'micasa.privado.es' ofrece un servicio de estafeta de correo (MTA) basado en el protocolo SMTP (Simple Mail Transfer Protocol), ¿cuál de las siguientes órdenes usaría?

a. telnet micasa.privado.es 25

b. dsniff micasa.privado.es smtp

c. telnet smtp micasa.privado.es

d. nmap micasa.privado.es smtp

4. Si queremos monitorizar todo el tráfico que se produce a un puerto TCP cerrado de cierto servidor en el que sospechamos que se proporcionan nombres de usuario y contraseñas para acceder a un servicio de alto valor para nuestros fines delictivos, ¿cuál de las siguientes herramientas nos podría ser de utilidad?

a. openvas

b. nmap

c. dsniff

d. Ninguna. Es imposible.

5. Para disminuir los riesgos que pueden producir las vulnerabilidades presentes en el sistema operativo de nuestras estaciones de trabajo, diseñamos una política de mantenimiento que impone la comprobación e instalación frecuente de actualizaciones de seguridad. Seleccione la afirmación que mejor describe el impacto que esta medida puede tener sobre el riesgo de nuestra instalación.

a. Esta contramedida está orientada a disminuir la pérdida de valor y por tanto disminuye el riesgo

global.

b. Aunque esta contramedida disminuye sólo la probabilidad de ataques por usuarios ocasionales o

aficionados pero no por expertos, conlleva una disminución del riesgo global.

c. Es una contramedida que disminuye la probabilidad de cualquier ataque pero no necesariamente la

disminución del riesgo global.

d. Es una contramedida que no genera más que sobrecostes.

6. Consideremos un stakeholder que actúa como proveedor de servicios de Internet y está preocupado por la vulnerabilidad de acceso físico a sus equipos de conexión troncal a la Internet. Sabe que una agencia gubernamental tiene acceso físico a las salas en que están instalados pero no sabría determinar si el riesgo que corre es alto o no. ¿Cuál de los siguientes razonamientos sería correcto transmitir a este señor en estas circunstancias?

a. El riesgo es alto porque el impacto sobre el bien es muy elevado, y con eso basta.

b. Como la agencia no tiene motivación especial para acceder a la sala e interrumpir el servicio, la

probabilidad de que eso suceda es despreciable, lo que hace que el riesgo sea bajo aunque el

impacto sobre el servicio sea muy alto.

c. El riesgo será bajo porque aunque es muy probable que la agencia intente bloquear el servicio, el

impacto que esto podría causar es muy bajo.

d. La agencia estatal nunca podría causar una interrupción de servicio.

7. Basin propone un esquema tabular para la estimación de probabilidades de ocurrencia de eventos que pueden conllevar pérdidas de valor en assets y, por tanto, ponderan los riesgos de seguridad de un sistema. Siguiendo este esquema, decimos que un evento tiene probabilidad media si:

a. La fuente de amenazas carece de motivación o capacidades para explotar la vulnerabilidad.

b. La fuente de amenazas tiene motivación y capacidad para explotar una vulnerabilidad, aunque los

controles establecidos pueden llegar a impedirlo.

c. La fuente de amenazas está muy motivada y tiene plena capacidad para explotar una vulnerabilidad

para la que disponemos de controles muy probados que protegen contra ese ataque.

d. La fuente de amenazas está muy motivada y tiene plena capacidad para explotar una vulnerabilidad

y no tenemos controles eficaces para contener el ataque.

8. En un Informe de Seguridad se indica "Contratación de personal certificado y con experiencia. Aplicación de medidas de seguridad actualizadas, de amplia aceptación y reconocibles por cualquiera. Revisiones periódicas de los sistemas de información certificadas por agencias externas". ¿A qué cree usted que se puede referir?

a. Relación de objetos de valor de la compañía.

b. Contramedidas para disminuir el riesgo de una amenaza que afecta al valor intangible de la

confianza de los clientes en la organización.

c. Conjunto de riesgos asociados al funcionamiento correcto de la compañía.

d. Aspectos de diferentes vulnerabilidades reconocidas de nuestro sistema.

9. Si queremos impedir que un fichero /etc/superseguro sea inmutable (no pueda borrarse ni cambiarse de nombre ni se pueda escribir nada en él ni se pueda enlazar desde otro)tendríamos que usar ...

a. chmod 9000 /etc/superseguro

b. unlink /etc/superseguro

c. chown nobody /etc/superseguro

d. chattr -i /etc/superseguro

10. Indica entre los siguientes pasos a llevar a cabo para realizar un análisis de riesgos el que consideres incorrecto:

a. Calcular las pérdidas anuales esperadas.

b. Estimar las probabilidades de que se produzcan los riesgos.

Estimar las probabilidades de que se produzcan dichos riesgos.

c. Identificar los assets.

d. Proyectar los ahorros de control diarios.

11. Una buena planificación de seguridad debe incluir un análisis cuidadoso de los riesgos. Un riesgo se distingue de cualquier otro evento del proyecto, según Rook, por varios aspectos que pueden ayudar a detectar esos riesgos. Señale cuál de los siguientes NO es un aspecto distintivo de un riesgo.

a. La pérdida asociada al evento.

b. El grado en que podemos alterar el resultado del evento.

c. La probabilidad de ocurrencia del evento.

d. La posibilidad de que se manifieste durante el funcionamiento del sistema.

12. Señale la única afirmación correcta relacionada con las amenazas entre las cuatro que se presentan:

a. Una amenaza es cualquier pérdida de valor generada por una fuente de amenazas.

b. Una amenaza es cualquier acción que da lugar a una vulnerabilidad.

c. Una amenaza se compone de una fuente de amenaza y de una acción, que representa una forma de

sacar partido de una vulnerabilidad.

d. Una amenaza se compone de una fuente y de una acción malintencionada y consciente que proviene

de una vulnerabilidad.

13. La seguridad computacional a menudo se divide en tres categorías maestras distintas, comúnmente llamadas Control Físico, Control Técnico y Control Administrativo. Estas tres grandes categorías ayudan en la definición de los objetivos principales de un plan de seguridad. En esta pregunta se le presentan diversos medios o actuaciones que debe hacer corresponder con aquélla de las tres categorías con la que mejor se corresponda en cada caso.

Software de auditoría de integridad de archivos. – Control Técnico

Estrategia de selección de personal. – Control Administrativo

Listas de control de acceso. – Control Técnico

Tarjeta inteligente. – Control Técnico

Guardia de seguridad. – Control Físico

Identificación de huella digital. – Control Físico

Autenticación a nivel de red. – Control Técnico

Plan de recuperación de desastres. – Control Administrativo

Circuito cerrado de cámaras. – Control Físico

Registro y control de personal. – Control Administrativo

14. En relación con un Riesgo de Seguridad, sólo hay una acción de las siguientes que NO podemos realizar en la práctica, ¿cuál?

a. Ignorarlo.

b. Limitarlo.

c. Identificarlo.

d. Eliminarlo.

15. En Gestión de la Seguridad, la preparación y estudio avanzado que nos permite saber si nuestra implantación satisface o no las necesidades de seguridad actuales y futuras constituye...

a. Las políticas de seguridad.

b. El análisis de riesgos.

c. La planificación.

d. Los controles físicos.

16. Sabemos que md5sum puede ser de ayuda para comprobar la integridad de los datos contenidos en uno o varios ficheros, elaborando a partir de cada uno un hash que se verá modificado cuando los contenidos se alteren. Sin embargo, para poder controlar modificaciones de los metadatos de los ficheros (fechas de modificación, propietarios, modos...) es más adecuado usar...

a. SHA1

b. chkrootkit

c. AIDE

d. ls -lR

17. Entre los métodos de identificación de los riesgos existe uno que es el uso de tormenta de ideas. En la relación de desventajas que presenta su utilización existe una que NO es correcta. Indícala.

a. La dinámica de la reunión puede sesgar los resultados.

b. Requiere entrenamiento.

c. Los resultados dependen de la experiencia de los participantes.

d. Mantiene a los participantes pasivos.

18. Administramos un sistema Linux y queremos impedir que un usuario sin privilegios de nuestro sistema realice una modificación accidental de un carácter de la versión encriptada de la contraseña del superusuario. Indique cuál de las siguientes alternativas identifica correctamente: El fichero en que se almacena ese dato, el modo de acceso recomendado para el mismo, y el tipo de ataque que representa esa amenaza.

a. /etc/group. u:r-,g:--,o:--. Denegación de acceso.

b. /etc/shadow. u:r--,g:r--,o:r--. Denegación de acceso.

c. /etc/shadow. u:rw-,g:r--,o:rw--. Denegación de acceso.

d. /etc/shadow. u:r--,g:---,o:---. Suplantación de identidad.

19. Un Plan de Seguridad debe identificar qué personas son responsables de adoptar comportamientos, tomar decisiones o implantar soluciones que garanticen el cumplimiento

de los Requisitos de Seguridad. Para cada elemento que aparece en la lista, seleccione quiénes serían los responsables idóneos en cada caso.

Supervisión de la creación, uso y eliminación de datos. – Responsables de información

Seguridad de los empleados. – Jefe de Personal

Cumplimiento de las medidas de seguridad por parte del personal. – Gestores

Seguridad de datos y procesamiento de datos. – Responsable de proyecto.

Acceso e integridad de los almacenes de información. – Administrador de Bases de Datos

Equipo de escritorio en el despacho del empleado. – Usuario de aplicaciones.

20. Si está tratando de identificar los stakeholders de un determinado sistema informático, indique cuál de las siguientes afirmaciones NO le ayudará en la tarea:

a. Un stakeholder no asigna valor al sistema, a sus componentes o a su funcionalidad.

b. Un stakeholder es una persona, o un grupo de personas con intereses similares.

c. Los stakeholders suelen incluir propietarios, administradores y usuarios del sistema.

d. Los stakeholders tienen capacidades, recursos, motivaciones.

21. Queremos configurar acceso SSH a un host remoto usando el mecanismo de par de claves pública privada. Para ello, hacemos uso de ssh-add y de ssh-agent para crear el par de claves y almacenar la que corresponda en el almacén de claves local. ¿Hemos de hacer algo más?

a. Debemos añadir la clave pública en el fichero ~/.ssh/authorized_keys del host remoto.

b. Debemos añadir la clave pública en el fichero ~/.ssh/authorized_keys de nuestra cuenta en local.

c. Debemos añadir la clave privada en el fichero ~/.ssh/authorized_keys del host remoto.

d. No hay nada más que hacer. Ya estaría listo.

22. Un plan de seguridad debe establecer la política sobre seguridad de la organización, es decir la declaración de alto nivel en la que se definen las metas y compromisos que la organización está dispuesta a asumir en materia de seguridad. Por ello, la declaración de la política de seguridad debe responder a tres preguntas fundamentales. Seleccione la pregunta que considere que no es fundamental para establecer una política de seguridad.

a. ¿Quién tiene permitido el acceso al sistema o la organización?

b. ¿Qué tipo de acceso se permite a cada usuario a cada recurso?

c. ¿A qué recursos del sistema o de la organización se permite acceder a un usuario?

d. ¿Qué formación técnica deben tener los usuarios que acceden al sistema o la organización?

23. Entre la relación siguiente de razones para llevar a cabo un análisis de riesgos cuando se está preparando un plan de seguridad hay una que no es correcta. Indicála.

a. Mejorar la base para decisiones.

b. Relacionar la misión de seguridad con los objetivos de marketing de la organización.

c. Identificar assets, vulnerabilidades y controles.

d. Justificar los gastos de seguridad.

24. Para implantar una protección contra modificación no deseada de los contenidos de una serie de ficheros importantes de nuestro sistema de ficheros hemos elaborado, usando MD5, una lista de pares (hash,fichero) que está almacenada en /etc/nocambiar.txt. La comprobación posterior de posibles modificaciones de los contenidos de uno o varios ficheros se podrá realizar con...

a. md5sum -new /etc/nocambiar.txt

b. md5sum /etc/nocambiar.txt

c. md5sum -c /etc/nocambiar.txt

d. find /etc/nocambiar.txt | md5sum

25. El análisis de los datos históricos de una organización que dispone de una base instalada de 1000 equipos de sobremesa indica que, en un periodo concreto suficientemente largo, 30 equipos sufrieron infección por un virus que hizo necesario reinstalar y reconfigurar completamente el equipo, para lo que se invirtieron 10 horas. Se estima que la pérdida de productividad y el coste de restauración del equipo, acumulados, representan 100 euros por hora. En estas circunstancias ¿cuál sería el indicador numérico de Exposición al Riesgo de infección por virus en este escenario?

a. 30 Euros.

b. 1000 Euros.

c. 30 minutos.

d. 3 Euros.

26. El marco de trabajo OCTAVE, creado por el Software Engineering Institute de la Universidad de Carnegie Mellon propone ocho pasos para guiar al gestor de proyectos o al analista de seguridad en la determinación de los riesgos de seguridad y la búsqueda y selección de controles adecuados para abordarlos. Ordene dichos pasos de acuerdo con la secuencia recomendada por OCTAVE:

1. Identificar el conocimiento de la empresa.

2. Identificar el conocimiento del área operativa.

3. Identificar el conocimiento del personal.

4. Establecer los requisitos de seguridad.

5. Localizar elementos de información de alta prioridad.

6. Realizar una evaluación de vulnerabilidades.

7. Elaborar un análisis de riesgos multidimensional.

8. Desarrollar una estrategia de protección.

27. El uso de Listas de comprobación como métodos de identificación de riesgos tiene múltiples ventajas entre las que se encuentran tres de las cuatro que le indicamos. Señale la única que NO es una ventaja.

a. Estandariza los resultados.

b. Rápido y fácil de utilizar.

c. Puede cubrir un amplio espectro de posibilidades.

d. Fomenta la creatividad.

28. La configuración de acceso SSH a un host remoto usando el mecanismo de par de claves pública privada desde una máquina de libre acceso instalada en un lugar público proporciona ventajas en términos de seguridad porque...

a. No usa ningún mecanismo de cifrado inseguro.

b. Nos permite acceder de forma más rápida y cómoda.

c. No proporciona ninguna, sino que compromete aún más la seguridad de nuestra cuenta.

d. No nos obliga a tener que introducir la contraseña, con el correspondiente riesgo de que alguien

que nos espía pueda sustraerla.

29. Un plan de seguridad debe establecer la política sobre seguridad de la organización, es decir la declaración de alto nivel en la que se definen las metas y compromisos que la organización está dispuesta a asumir en materia de seguridad. La declaración de la política de seguridad debería especificar tres de los cuatro aspectos que se presentan a continuación. Señale cuál de ellos sobra...

a. Los objetivos de seguridad de la organización.

b. La determinación quién o quiénes son responsables de la seguridad.

c. El conjunto de inversiones necesarias para garantizar la seguridad.

d. El grado de compromiso de la organización con la seguridad.

30. En Gestión de la Seguridad, el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma constituye...

a. La política de seguridad.

b. Los controles físicos.

c. La planificación.

d. El análisis de riesgos.

31. El marco de trabajo elaborado por Basin propone siete pasos para guiar al analista de seguridad en la determinación de los riesgos de seguridad y la búsqueda y selección de controles adecuados para abordarlos. Ordene dichos pasos de acuerdo con la secuencia recomendada por Basin:

1. Identificar los objetos de valor.

2. Identificar las vulnerabilidades.

3. Identificar las amenazas.

4. Planificar contramedidas.

5. Determinar probabilidades.

6. Determinar el impacto de cada amenaza.

7. Estimar los riesgos de seguridad.

32. Consideremos un sistema informático que contiene un servidor web. ¿Cuál de las siguientes se puede considerar una vulnerabilidad?

a. Un cambio de configuración fortuito en los ficheros de configuración del servidor.

b. Un defecto del sistema operativo que permite obtener permisos de superusuario.

c. Una pérdida de datos de la base de datos del servidor.

d. Una saturación del servicio por aumento desmesurado del número de conexiones.

33. En el dominio de Planificación de Seguridad, la Política de Seguridad, la Identificación, la Calificación, el Seguimiento, la Garantía y la Protección Contínua son:

a. Seis dominios de seguridad marcados por el Departamento de Defensa de los Estados Unidos.

b. Ejemplos de controles que deben implantarse en una organización segura, según el DoD americano.

c. Los seis requisitos de seguridad esenciales que marca el TCSEC del Departamento de Defensa americano.

d. Las seis necesidades de seguridad que tiene cualquier organización, según el TCSEC elaborado por el DoD americano.

34. Una forma de clasificación de los controles de seguridad es la que propone dividirlos en:

1. Aquéllos que tratan de evitar que se produzca un suceso que pueda amenazar la seguridad del

sistema, denominados controles preventivos

2. Aquéllos que, cuando fallan los anteriores, tratan de localizar cuanto antes cualquier suceso que

pueda amenazar la seguridad del sistema, denominados controles de detección

3. Aquéllos que, asumiendo que se puede dar un suceso que pueda amenazar la seguridad del sistema, tratan de facilitar la vuelta al funcionamiento normal y seguro cuanto antes, denominados controles correctivos.

Atendiendo a estas definiciones, se le propone clasificar los siguientes controles en alguna de las tres

categorías definidas anteriormente:

1. Uso de swatch para análisis periódico de ficheros de bitácora del sistema controles preventivos.

2. Instalación de un software de seguridad que impide accesos no autorizados al sistema controles

preventivos.

3. Implantación de un sistema de copias de seguridad y restauración de ficheros críticos controles

correctivos.

35. Seleccione la definición que mejor se corresponde con el concepto de Requisitos de Seguridad desde el punto de vista de la Planificación de la Seguridad. (Sólo una es la correcta)

a. El conjunto de necesidades de seguridad que tiene la organización.

b. El conjunto de normas de seguridad que establece un estándar de seguridad o una agencia estatal.

c. Las demandas de prestaciones o funcionales que deben exigirse a un sistema para garantizar un nivel deseado de seguridad.

d. Los controles que deben aplicarse para lograr un nivel de seguridad determinado.

36. Cuál de los siguientes no es un objetivo de los procesos de mediciones de seguridad de la información:

a. Comunicar valores de seguridad a la organización.

b. Proporcionar estados de seguridad que guíen las revisiones del SGSI, facilitando mejoras a la

seguridad.

c. Disponer de datos para el departamento de contabilidad de la organización.

d. Evaluar la efectividad de la implementación de los controles de seguridad.

37. Indica cuál de las siguientes es una actividad fundamental para una valoración típica de los riesgos:

a. No consideración del efecto de los riegos

b. Priorización de los riesgos que no necesitan ser mitigados

c. Obtención de las vulnerabilidades y amenazas

d. Elaboración de una lista con los riesgos menos importantes

38. Una aplicación exige del usuario la presentación de un certificado válido pero un usuario presenta uno que podría haber sido sustraído a otro usuario que comunicó a la autoridad de certificación el hecho para que revocase el certificado. ¿Cómo podría determinar la aplicación si el certificado está revocado?

a. Debe enviar el certificado a la CA para que compruebe con sus listas de revocación si está revocado.

b. Debe comprobar que el certificado es correcto y está firmado por una CA reconocida.

c. No hay que hacer nada, porque el propio certificado contiene información sobre la revocación.

d. Debe consultar en su lista de certificados revocados.

39. Queremos usar chroot para configurar una cuenta de usuario de modo que sólo se tenga acceso, recursivamente, a los ficheros contenidos en la carpeta del usuario. Una vez realizada la configuración adecuada del intérprete de órdenes asociado a esa cuenta queremos que el usuario tenga disponible la órden 'ls'. Indique cuál de las siguientes alternativas nos garantizará que esto esposible en cualquier circunstancia. NOTA: Suponga que la carpeta de usuario es /home/u1 y que /home/u1/bin es la ubicación, contenida en el PATH, en que se encuentran las órdenes que el usuario podrá ejecutar.

a. Copiaremos todo el sistema de ficheros en /home/u1

b. Basta con enlazar /bin/ls a /home/u1/bin y cambiar los modos.

c. Enlazaremos /bin/ls a /home/u1/bin, comprobaremos los modos de acceso y las bibliotecas

dinámicas que usa la orden, enlazando las que corresponda en la ubicación accesible para el usuario.

d. No hay que hacer nada especial.

40. Casi todos los autores coinciden en que un plan de seguridad...

a. No tiene por qué incluir la descripción de un plan de mejora.

b. Debe contener una descripción de la situación futura del sistema respecto a la seguridad

c. Debe identificar y organizar las actividades de seguridad para un sistema de computación.

d. Una vez descrito dicho plan de seguridad no hay que modificarlo