PRUEBA SELECTIVA PARA CUBRIR CON CARÁCTER TEMPORAL UN PUESTO DE RESPONSABLE AREA SEGURIDAD EN LA ENTIDAD PUBLICA ARAGONESA DE SERVICIOS TELEMÁTICOS

CONVOCADA POR RESOLUCIÓN DE 18 DE JULIO DE 2018, DE LA DIRECTORA GERENTE DE LA ENTIDAD PUBLICA ARAGONESA DE SERVICIOS TELEMÁTICOS. (Oferta 02-2018-007672).

1. En la gestión de seguridad ITIL, esta es:

a) Un proceso estático con actividades de planificación, implementación y puesta en marcha
b) Un proceso continuo en el que se distinguen actividades de control, planificación, implementación, evaluación y mantenimiento
c) Un proceso discreto en el que hay actividades de control, mantenimiento y auditoría

2. De acuerdo a los principios de CoBIT:

a) La gestión IT debe obviar las partes no IT de la empresa
b) Hay que cubrir la empresa de principio a fin
c) Nunca es necesario optimizar el uso de los recursos

3. En iOS 10, las claves de cifrado de los elementos más sensibles del sistema como 'keychains' y claves de ficheros se encuentran protegidos de la siguiente manera:

a) Almacenadas en un fichero de texto propiedad de root y sin permisos de acceso ni para grupo ni para otros
b) Además de lo anterior este fichero se encuentra cifrado con una clave AES de 512 bits
c) Las claves se encuentran almacenadas en el 'Secure Enclave' y nunca salen en "claro" de ese ámbito de seguridad

4. Indica cuál de estas métricas no se emplearía dentro de la gestión de disponibilidad en ITIL:

a) Tiempo Medio entre Fallos (MTBF)
b) Tiempo Medio en Restaurar Servicios (MTRS)
c) Tiempo Medio de Carga de Servicio (TMCS)

5. ¿Cuál es la fecha de entrada en vigor del actual Reglamento General de Protección de Datos?

a) 24 de mayo de 2016
b) 25 de mayo de 2018
c) 1 de enero de 2017

6. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento notificará siempre

a) A la autoridad de control competente
b) A la autoridad de control competente y al interesado cuyos datos han sido comprometidos
c) Al interesado cuyos datos han sido comprometidos

7. En caso de detección de un equipo o conjunto de equipos comprometidos en un ataque de robo de información (APT, Advanced Persistent threat)

a) A la mayor brevedad, realizar un borrado seguro del disco duro, o al menos cerrar el acceso a la red de dicho equipo para evitar la comunicación con los servidores de mando y control del atacante
b) Comenzar un proceso de monitorización exhaustiva de dicho equipo y trazar un plan de análisis forense para averiguar el alcance del ataque
c) Desconectar de la red la máquina o máquinas bajo ataque y situarlas en cuarentena para copiar su información y analizarla

8. Los sistemas implicados en la gestión de recursos humanos por parte de la administración (función pública), ¿se encuentran dentro del ámbito del ENS?

a) Verdadero
b) Falso
c) Únicamente para procesos de selección de funcionarios de carrera y funcionarios interinos

9. Un sistema de back-office (no visible desde el exterior) utilizado para, por ejemplo, gestionar procedimientos sancionadores de los ciudadanos, ¿quedaría dentro del alcance del ENS?

a) Verdadero
b) Falso
c) Depende de la cuantía de la sanción

10. En un ataque XSS almacenado, el script javascript se encuentra …

a) En un enlace proporcionado por el atacante vía email, whatsupp, …
b) Guardado en la base datos de la que se alimenta el servidor web
c) Almacenado en el .bashrc del usuario asociado al servidor web

11. El ámbito de aplicación del Esquema Nacional de Seguridad es:

a) Las Administraciones Públicas, entendiendo por tales la Administración General del Estado, las Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas
b) Los ciudadanos en sus relaciones con las Administraciones Públicas y las relaciones entre las distintas Administraciones Públicas
c) Todas las anteriores

12. El análisis de riesgos considera los siguientes elementos:

a) Activos, amenazas y salvaguardas
b) Activos, pasivos y amenazas
c) Impactos, riesgos y defensas

13. En Android, qué fichero almacena los permisos de acceso del .apk correspondiente:

a) AndroidManifest.xml
b) Tanto los ficheros '.dex' como '.smali'
c) El fichero BroadCast.receivers

14. El análisis de riesgos determina impactos y riesgos:

a) Los impactos reflejan daños absolutos con independencia de su probabilidad y el riesgo estima la probabilidad de la ocurrencia de dichos impactos
b) Los impactos reflejan daños ocurridos y el riesgo determina su probabilidad
c) Los impactos son circunstanciales y ocurren rara vez por lo que su riesgo es bajo

15. De acuerdo al ENS, los sistemas informáticos

a) De nivel alto deberán contar con un plan de continuidad de servicio y un plan de pruebas periódicas de continuidad
b) De nivel medio y alto deberán contar con un plan de continuidad de servicio y, además, en el caso de nivel alto, un plan de pruebas de periódicas de continuidad
c) De nivel bajo, medio y alto deberán contar con un plan de continuidad de servicio y un plan de pruebas periódicas de continuidad

16. De acuerdo al ENS, los sistemas informáticos de la administración pública deberán contar con un análisis de impacto de la interrupción de su servicio. Este análisis permitirá determinar: a) Los requisitos de disponibilidad de cada servicio medidos como el impacto de una interrupción durante un cierto periodo de tiempo y b) Los elementos que son críticos para la prestación de cada servicio.

a) Sistemas informáticos de todos los niveles: bajo, medio y alto
b) Sistemas informáticos de nivel: medio y alto
c) Sistemas informáticos de nivel: alto.

17. De acuerdo al ENS, las copias de seguridad de los registros de actividad de un sistema de categoría alta serán protegidos de manera que:

a) Se determinará el periodo de retención de las copias y se asegurará la fecha y hora
b) Las copias no podrán ser modificados ni eliminados por el personal no autorizado
c) Todas las anteriores

18. ¿En qué capa se implementa el protocolo Transport Layer Security de acuerdo al modelo OSI?

a) Enlace
b) Transporte
c) Aplicación

19. Cuál de las siguientes medidas no debería ser recomendada en una configuración de seguridad para los empleados en usos corporativos

a) Configuración y uso de VPNs
b) Uso de sistemas de ficheros sin cifrado
c) Utilización y verificación de copias de seguridad

20. La concienciación en ciberseguridad requiere formar a los empleados en temas como:

a) Ingeniería social, gestión de documentación, contraseñas seguras y métodos de autenticación
b) Criptografía avanzada y técnicas de pentesting
c) Gestión de información únicamente

21. El esquema nacional de interoperabilidad indica que los estándares que deban usarse serán:

a) Aquellos que faciliten la implementación y mantenimiento de los sistemas informáticos
b) Abiertos en general y de forma completaría, estándares que sean de uso mayoritario por parte de la ciudadanía
c) Siempre abiertos para que los ciudadanos nunca sean discriminados por su elección tecnológica

22. La norma técnica de interoperabilidad de Documento Electrónico para las administraciones públicas tiene como objeto:

a) Establecer los componentes del documento electrónico, contenido, en su caso, firma electrónica y metadatos, así como la estructura y formato para su intercambio
b) Establecer las consideraciones relativas a la seguridad del documento, incluido su posible cifrado
c) Las dos anteriores

23. El acceso a la red SARA se realizar a través de Puntos de Presencia PdP y entre estos se pueden distinguir:

a) Ciudadanos y organismos oficiales
b) Centros de Proceso de Datos (CPD) de SARA, ciudadanos y ventanillas únicas empresariales
c) Centros de Proceso de Datos (CPD) de SARA, Prestadores de servicios de certificación y centros externos de monitorización

24. Según el ENI, en el intercambio de Expedientes Electrónicos o Documentos Electrónicos entre Administraciones públicas que suponga transferencia de custodia o traspaso de responsabilidad de gestión que deba conservarse permanentemente, ¿qué órgano o entidad es responsable de comprobar la autenticidad e integridad en dicho momento de intercambio?

a) La entidad transferidora
b) La entidad receptora
c) No está especificado

25. Según el ENI, los metadatos asociados a un Documento Electrónico o a un Expediente Electrónico, ¿pueden ser modificados con posterioridad?

a) Si
b) No
c) No, a excepción de modificaciones necesarias para la corrección de errores u omisiones en el valor inicialmente asignado

26. A la hora de aprovecharse de la vulnerabilidad SQ injection, generalmente el navegador web juega las veces de:

a) Herramienta de ataque
b) Superficie de ataque
c) Vector de ataque

27. En ausencia de Cross-Site Scripting, XSS, el ataque Cross-Site Request Forgery, CSRF, puede ser evitado con cuál de las siguientes defensas:

a) Same origin policy
b) Aceptar únicamente peticiones POST
c) Utilizar una cookie secreta

28. Cómo se clasificaría el riesgo de un "cambio de legislación o normativa" en la siguiente clasificación:

a) Acciones humanas
b) Fallos del sistema o tecnologías
c) Eventos externos

29. Para evitar la amenaza de pharming qué elemento debemos proteger prioritariamente

a) El servidor de nombres de dominio
b) El cifrado de la red inalámbrica
c) El control de acceso a los sistemas de información que dan soporte a los servicios

30. En un sistema operativo microkernel

a) Un fallo en un módulo puede colgar el sistema
b) Los servicios corren en modo kernel
c) Es necesario disponer de mecanismos de comunicación entre procesos para los servicios del sistema operativo

31. De acuerdo a la recomendación X.800, Security Architecture for SOI, indique cuales son mecanismos de seguridad:

a) Firma digital, control de acceso, control de routing
b) Autentificación, gestión de usuarios, no-repudio
c) Integridad conexión, encriptación, no-repudio

32. Al emplear defensa en profundidad:

a) Se dispone de una única capa de seguridad muy profunda que no permite al atacante tomar el control del sistema
b) Se emplean múltiples capas de seguridad para tener redundancia
c) Se emplea el mismo sistema de seguridad en las distintas capas del modelo OSI

33. En un algoritmo de cifrado simétrico:

a) El remitente y el destinatario no necesitan proteger bien la clave
b) Es recomendable que el remitente y el destinatario compartan la clave
c) El remitente y el destinatario necesitan siempre compartir la clave para cifrar y descifrar un mensaje entre ellos

34. ¿Cuál es la diferencia entre el cifrado en bloque y en flujo?

a) El cifrado en bloque utiliza claves privadas mientras que el cifrado en flujo emplea claves públicas
b) El cifrado el bloque cifra un conjunto de elementos en un bloque en una única operación mientras que el cifrado en flujo cifra elemento a elemento
c) El cifrado en bloque genera una cadena de elementos completamente aleatorios para cifrar y el cifrado en flujo utiliza el mensaje para generar la clave

35. Los ataques de seguridad pasivos y activos se pueden distinguir porque:

a) En los ataques activos el atacante modifica la transmisión de datos y genera datos falsos y en los pasivos sólo monitoriza el tráfico
b) Los ataques pasivos son muy difíciles de detectar al contrario que los activos
c) En los ataques pasivos se capturan los datos únicamente para ser observados y no se modifican mientras que en los activos siempre se modifican

36. El RFC 3748 define los protocolos de autenticación extensibles, EAP, y estos están compuestos por las capas:

a) Métodos de autenticación, EAP y capa de enlace
b) Aplicación, transporte y enlace
c) EAP no utiliza capas

37. De las siguientes opciones de configuración cuales considerarías para mejorar la protección de una distribución de Linux para un servidor:

a) Instalar Mandatory Access Control, MAC, como por ejemplo mediante SELINUX
b) Instalar GNOME frente KDE
c) Proteger frente a escritura el directorio /lib

38. Si un atacante tiene acceso físico a un servidor Linux que medida es la mínima necesaria para proteger el acceso a root del sistema

a) Ninguna, no es necesario
b) Utilizar un password muy fuerte según la NIST-800
c) Configurar adecuadamente la BIOS y protegerla con password

39. Para establecer un Área de Conexión, la Red SARA recomienda utilizar una zona desmilitarizada, DMZ, con 2 cortafuegos porque:

a) Es un esquema obsoleto y la ley debería actualizarse
b) Una DMZ con 2 cortafuegos es en principio más segura que una DMZ con un único cortafuegos
c) Una DMZ sólo puede implementarse con 2 cortafuegos

40. En un sistema Linux, determine si los siguientes módulos de Linux-PAM (Pluggable Authentication Modules for Linux) se emplean para mejorar la seguridad en los passwords:

a) pam_cracklib y pam_unix
b) pam_permit y pam_unix
c) pam_permit y pam_shells

41. SSL está compuesto por:

a) Un protocolo único diseñado para ofrecer una conexión segura extremo a extremo
b) Un protocolo a nivel de aplicación para ofrecer conexiones seguras extremo a extremo
c) Al menos 2 capas de protocolos en las que se establece conexiones y sesiones

42. La herramienta de detección de amenazas Suricata permite:

a) Responder ataques mediante el lanzamiento de un contraataque de denegación de servicio al atacante
b) Detección de intrusos en tiempo real y monitorización de red
c) Detección de ataques sin firma

43. Para responder de manera eficaz a incidentes se deberá:

a) Definir un plan de respuesta a incidentes, contener los daños y minimizar los riesgos
b) Apagar inmediatamente todos los sistemas para evitar más problemas
c) Notificar a todos los usuarios del incidente

44. En un servidor de correo podemos evitar spoofing utilizando:

a) Sender Policy Framework (SPF)
b) Receiver ID
c) SMTP TLS

45. A la hora de realizar un clonado de un disco para hacer un análisis forense:

a) Debe extraerse el disco y clonarlo con ayuda de otro sistema operativo ya que no modificará el disco
b) Debe emplearse un Hardware Write Blocker para garantizar que el disco no puede ser modificado
c) Lo más importante antes del clonado es leer el disco para comprobar si se han perdido datos

46. Ante el fenómeno Bring your own device, BYOD, indica cuales de las siguientes prácticas son recomendables para su implantación (marcar tantas como sea necesario):

a) Uso de la virtualización y del cloud
b) Uso de la paralelización
c) Uso del aislamiento (sandboxing)

47. Es posible realizar recuperación forense de datos sobre:

a) Medios de almacenamiento volátil y no volátil
b) Medios de almacenamiento no volátil
c) Medios de almacenamiento no encriptados

48. Indique cuál de las siguientes afirmaciones es verdadera:

a) Un plan de continuidad del negocio, BCP, debe incluir un plan de recuperación de desastres, DRP.
b) Un plan de recuperación de desastres, DRP, debe incluir un plan de continuidad del negocio.
c) El plan de continuidad del negocio, BCP, y el plan de recuperación de desastres, DRP, deben realizarse de manera completamente independiente

49. Cuál es el punto débil de las APT's utilizado por los analistas en seguridad para detectarlas:

a) Utilizan malware cuyas firmas son muy conocidas y se pueden consultar en bases de datos
b) Afectan severamente el rendimiento de los equipos afectados, importunando severamente a los usuarios de los equipos
c) Los equipos infectados se conectan regularmente a un servidor "mando de control", un profundo y correlacionado análisis de los equipos de la institución puede resultar señalando al mando de control

50. Supongamos el uso plataformas de compartición de documentos en Nube Pública (p.e. Dropbox, Google Drive, …) y su uso seguro institucional. Con respecto a los datos allí alojados ¿qué legislación aplica con respecto a la protección de datos y quién es responsable?

a) El cliente es el responsable y la normativa aplicable al cliente y al prestador del servicio es la legislación española sobre protección de datos (LOPD)
b) Depende del país de origen de la empresa proveedora de los servicios en nube
c) Ninguna de las anteriores

PREGUNTAS DE RESERVA

51. ¿A qué se refieren las siglas PDCA en un SGSI?

a) Es una estrategia de mejora continua, basada en 4 pasos planificar, hacer, verificar, actuar

b) Es un documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones

c) Es el Plan Dinámico de Control de los Activos de un SGSI

52. De acuerdo al Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica, los sistemas informáticos que presten un servicio público deberán sincronizarse:

a) Con la hora del Real Instituto y Observatorio de la Armada y, cuando sea posible, con la hora oficial a nivel europeo

b) Con la hora oficial a nivel mundial

c) Con la hora oficial de cada comunidad autónoma ya que el territorio español cubre varias franjas horarias

53. Meltdown y Spectre son

a) Riesgos

b) Ataques

c) Vulnerabilidades

54. En que consiste defacement

a) Mails falsos, mensajes de texto o sitios web creados para ser muy parecidos a los utilizados por compañías legítimas. Estos elementos son enviados por el atacante para robar información personal o financiera

b) Conseguir la redirección desapercibida de una URL legítima a un sitio ilegitimo controlado por el atacante para un equipo o conjunto de equipos

c) Deformación o cambio de la apariencia de una web legítima de manera intencionada por parte de un atacante

55. ¿Cuál de los siguientes es un protocolo de red que se encarga de recolectar de los distintos actores de la red información sobre el tráfico que más tarde son enviados a un servidor central, que más tarde son utilizados por algunas herramientas SIEM para detección de trafico anómalo?:

a) Netflow

b) NetMonitor

c) NetInspector