Test Tema 128 #1

Actualizado el 13/04/2025

1. Seleccione la respuesta correcta sobre las estrategias de recuperación:

a) Los Cold Sites son instalaciones parcialmente configurados, que permiten la recuperación en menos de una semana.

b) Las instalaciones redundantes permiten una recuperación inmediata ante una interrupción.

c) Los Hot Sites tienen un coste menor que los Cold Sites.

d) La configuración más adecuada para un Warm Site es de mirroring.

2. En el ámbito de la continuidad de negocio una operación clasificada como vital:

a) Puede realizarse manualmente por un periodo breve de tiempo.

b) Tiene mayor tolerancia a las interrupciones que una clasificada como crítica.

c) Ninguna de las anteriores.

d) A y B.

3. Un plan de contingencia:

a) previene incidentes

b) se aplica después de un interrupción para recuperar los servicios críticos

c) se aplica después de un interrupción de servicios y activos para auditar los daños

d) después de un interrupción para corregir los daños

4. Para determinar la estrategia de continuidad, es necesario conocer:

a) los tiempos de exposición a las interrupciones

b) los sistemas y activos críticos de la organización

c) el avance de las iniciativas en el ámbito de la continuidad

d) cuando tomar la decisión de activar al plan de continuidad

5. Para comunicar al equipo sobre el SGCN, se realiza a través:

a) Metadatos

b) Recepción, almacenado y respuesta de comunicaciones con stakeholdres

c) utilización sistema de aviso de llamadas por la conformidad de negocio

d) Utilización de documentación, aunque esté desactualizada

6. ¿Qué tendencias de enfoques de alcance del SGCN existen?

a) activos y pasivos

b) directos e indirectos

c) activos y pasivos, orientado a procesos

d) activos y pasivos, directos e indirectos

7. La política del SGCN se debe caracterizar por, (señale la incorrecta):

a) Incluir la posibilidad de la mejora continua

b) Estar en línea con los objetivos de la organización

c) Definir la estructura que establezca los objetivos de continuidad de negocio

d) Incluir la obligatoriedad de los requisitos de SGCN

8. El alcance del SGCN debe tener en cuenta:

a) Determinar la magnitud y coste del proyecto, así como su viabilidad futura

b) Definir qué elementos de la organización van a ser el foco de la mejora continua

c) Requerir de la colaboración de todos los departamentos implicados

d) Todos los anteriores

9. ¿Cuál de las siguientes opciones contribuye mejor a un plan de continuidad de negocio eficaz?

a) La documentación se distribuye a todas las partes interesadas

b) La planificación involucra a todos los departamentos de usuarios

c) El plan se ha aprobado por la alta dirección

d) El plan se ha auditado por un auditor externo

10. En el ENS la medida de Plan de Continuidad aplica alnivel:

a) Alto

b) Medio

c) Bajo

d) Alto y medio

11. Cuál de las siguiente es una norma que aplique en relación a los planes de continuidad de negocio:

a) ENI

b) ISO 22301

c) ISO 9001

d) Ninguna de las anteriores

12. La ISO 22301 establece como parte de la información que debe incorporarse al Plan de Continuidad la siguiente:

a) El alcance.

b) La lista de requisitos legales y normativos.

c) El análisis de impacto en el negocio.

d) Todas las anteriores son ciertas.

13. En el contexto de los planes de contingencia y continuidad del negocio, el parámetro RTO nos determina:

a) El tiempo que un proceso puede permanecer caído antes de que se produzcan consecuencias desastrosas para nuestra empresa

b) El nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada, aunque el nivel de servicio no sea el óptimo

c) El tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado

d) El tiempo que hemos estado sin fallos en el sistema

14. La norma ISO 22301 tiene su precedente en la:

a) ISO 9001

b) ISO 27001

c) BS 25999

d) Ninguna de las anteriores

15. El “Plan” cuyo objetivo es conseguir la continuidad en las funciones estratégicas de una organización desempeñadas en sus instalaciones corporativas se denomina:

a) Plan de continuidad de operaciones.

b) Plan de continuidad de negocio.

c) Plan de contingencia.

d) Plan de emergencia.

16. El alcance de un Sistemas de Gestión de la Continuidad del Negocio:

a) debe dotar de recursos al SGCN

b) debe fomentar la mejora continua

c) debe asignar responsables del SGCN

d) debe identificar las necesidades de los stakeholders

17. Los equipos de continuidad de negocio deben: 1.Comunicar a las partes interesadas y autoridades en caso necesario; 2.Activar la respuestas de continuidad de negocio adecuadas; 3.Monitorizar los efectos del incidentes y de las respuestas; 4.Promover y difundir la mejora continua.

a) 1, 2, 3, 4

b) 2, 3, 4

c) 1, 2, 3

d) 3, 4

18. La gestión de la continuidad de negocio está normalizada por la Norma Internacional:

a) ISO 22301:2019.

b) ISO 22301:2018.

c) ISO 27001:2013.

d) ISO 22301:2014.

19. ¿Qué tipo de revisión NO se debe hacer en las pruebas de continuidad?

a) Documental

b) Integración

c) Sistemas

d) Aceptación

20. ¿Qué debe existir obligatoriamente dentro de un Plan de Continuidad del Negocio?

a) proceso de gestión de competencias

b) proceso de evaluación por parte de la gerencia

c) el alcance

d) el coste del plan de continuidad

21. En el ámbito de la continuidad de negocio, el "objetivo de prestación de servicios" se define como:

a) El tiempo que una organización puede esperar desde el punto de fallo hasta la restauración de los servicios o aplicaciones críticas.

b) El nivel de servicios a proveer durante el modo de proceso alterno.

c) Ninguna de las anteriores.

d) A y B.

22. El intervalo o la latencia de tiempo entre la última transacción de datos confirmada antes del error y los datos más recientes recuperados después del error se denomina:

a) Objetivo de tiempo de recuperación (RTO).

b) Objetivo de punto de recuperación (RPO).

c) Objetivo de nivel de recuperación (RLO).

d) Objetivo de datos de recuperación (RDO).

23. ¿Cuál es la fuente principal para calcular los tiempos estimados de recuperación de las actividades (RTO)?

a) Plan de Respuesta ante incidentes.

b) Pruebas de stress.

c) Plan de Comunicación de crisis.

d) Análisis de impacto en el negocio.

24. En relación con los centros de tratamiento de información y la recuperación ante posibles desastres, el tiempo que un proceso permanecerá detenido antes de que su funcionamiento sea restaurado, se conoce como:

a) RPO

b) RTO

c) MTD

d) ROL

25. El RPO define:

a) El tiempo máximo que se acepta que este el negocio no operativo.

b) La cantidad de perdida de dato durante un desastre que la empresa considera tolerable.

c) El Tiempo máximo tolerable de caída.

d) El real punto objetivo.

26. ¿Qué determinan los RTOs?

a) El volumen de datos que se perderán después de un desastre o contingencia.

b) La frecuencia en que hay que realizar los backups.

c) El tiempo máximo que se establece desde la última copia de seguridad.

d) El tiempo máximo aceptable para recuperar los procesos críticos después de un desastre o contingencia.

27. Todos los planes de continuidad del negocio deben ser concisos y accesibles para aquellos con responsabilidades definidas dentro de los mismos. Puede haber varios planes de continuidad del negocio que de forma conjunta cubran las necesidades del negocio. ¿Qué debe contener cada plan?

a) El procedimiento de respuesta que incluya detalles sobre las acciones y tareas que la dirección debe llevar a cabo.

b) El procedimiento de respuesta para abordar las cuestiones a todos los niveles: opciones estratégicas, tácticas u operacionales.

c) El procedimiento de respuesta debería incluir la gestión de cuestiones de asistencia social cuando sea apropiado.

d) El procedimiento de respuesta debería incluir quién tiene la responsabilidad y cuál es el método para activar y desactivar los planes.

28. Respecto a un plan de contingencia:

a) suponen una visión global para garantizar la continuidad del negocio, e incluye la formación del equipo

b) suponen una visión global para garantizar la continuidad del negocio, y se basa en la norma ISO 27.001 y 27.002

c) suponen una visión detallada para garantizar la continuidad del negocio, e incluye la formación del equipo

d) suponen una visión detallada para garantizar la continuidad del negocio, e incluye análisis de activos criticos

29. Un sitio frio de respaldo se caracteriza por:

a) Un coste reducido de preparación ante desastres

b) Altos costes de implementación y mantenimiento

c) Un tiempo reducido de recuperación

d) ninguna de las anteriores

30. El Plan de Continuidad de Negocio se encuadra dentro de ITILv3:

a) Diseño del servicio

b) Estrategia del servicio

c) Operación del servicio

d) Mejora continua

31. Indique cuál de los siguientes es un documento mínimo reclamado por la ISO 22301 de gestión de la continuidad del negocio:

a) Procedimiento para el control de la información documentada.

b) Estructura de respuesta a incidentes.

c) Los contratos y acuerdos de nivel de servicio con los proveedores.

d) Formación y plan de sensibilización.

32. Las imágenes se utilizan para:

a) la realización de un backup típico

b) almacenar datos antiguos para asegurar la compatibilidad

c) para recuperar datos en caso de desastre

d) todas las anteriores

33. En el contexto de la gestión de la continuidad del negocio, según la norma ISO 22301, ¿a qué se corresponde el acrónimo BIA?

a) Business Impact Analysis

b) Business Independent Analysis

c) Business Impact Assesment

d) Business Incident Assesment

34. ¿Cuál de los siguientes planes no formaría parte de un Plan de Contingencias?

a) Plan de emergencia

b) Plan de sistemas

c) Plan de recuperación

d) Plan de respaldo

35. Un parámetro manejado para definir la recuperación de un sistema de información ante un impacto es:

a) Recovery Time Objective.

b) Recovery Plan Objective.

c) Occupant Emergency Plan.

d) Business Recovery Plan.

36. En el ámbito de la continuidad de negocio, el Punto de Recuperación Objetivo o "Recovery Point Objective RPO":

a) Cuantifica la pérdida de datos aceptable en caso de interrupción.

b) Indica el punto más alejado en el tiempo en el que es aceptable recuperar los datos.

c) Es la cantidad de tiempo permitida para la recuperación de un recurso o función de negocio después de que ocurre un desastre.

d) A y B.

37. La Estrategia Nacional de Ciberseguridad 2019 se sustenta y se inspira en los siguientes principios rectores:

a) Inversión, Corrección, Planificación y Puertas abiertas.

b) Confidencialidad, Integridad, Disponibilidad y Autenticidad.

c) Unidad de acción, Anticipación, Eficiencia y Resiliencia.

d) Innovación, Investigación, Despliegue y Uso de sistemas analógicos.

38. En los planes de contingencia es necesario desarrollar:

a) El Plan de Crisis o de incidentes.

b) Los planes operativos de recuperación de entornos.

c) Los procedimientos técnicos de trabajo.

d) Todas las anteriores son ciertas.

39. La fase de planificación de un Sistemas de Gestión de la Continuidad del Negocio (SGCN) abarca:

a) El contexto, el liderazgo, los objetivos, las competencias, la comunicación y la documentación.

b) El contexto, el liderazgo, los objetivos, las competencias y la documentación.

c) El contexto, el liderazgo, los riesgos externos, las competencias, la comunicación y documentación.

d) Los sistemas de información, el liderazgo, los objetivos, las competencias, la comunicación y documentación.

40. La implantación de un Sistema de Gestión de la Continuidad del Negocio es un proceso de mejora:

a) Puntual.
b) Cíclico.
c) Lineal.
d) Inabordable.

41. El RTO define:

a) La cantidad de perdida de dato durante un desastre que la empresa considera tolerable.

b) El Tiempo máximo tolerable de caída.
c) La real transaccion objetiva.
d) El tiempo máximo que se acepta que este el negocio no operativo.

42. En el BIA, ¿quá actividad se realiza?

a) Evaluar el riesgo e impacto de una interrupción
b) Evaluar si se pueden acceder a los datos
c) Evaluar el cumplimiento de la estrategia
d) Evaluar la respuesta de la contigencia

43. Llevar a cabo una Plan de Continuidad de negocio permite:

a) Minimizar el impacto de los incidentes.
b) Facilitar la operación de funciones críticas.
c) Mejorar el tiempo de reacción.
d) Todas las anteriores son ciertas.

44. Seleccione el documentos NO obligatorio para la implementacion de ISO 22301:

a) Procedimientos de recuperación
b) Procedimientos de identificacion de riesgos y desastres naturales
c) Análisis del impacto en el negocio
d) Planes de continuidad del negocio

45. A partir de la realización de la última copia de seguridad, se determina:

a) el RTO
b) el RPO
c) el MTD
d) Ninguno de los anteriores

46. Dentro de los sistemas de protección contra fallos basados en la redundancia de hardware, existen componentes que se replican para proporcionar alta disponibilidad de los sistemas. ¿Cuál de los siguientes NO se incluye en estos elementos redundados?

a) Fuentes de alimentación.
b) Elementos de memoria caché.
c) Dispositivos de conexión a la red.
d) Dispositivos de almacenamiento.

47. ¿Qué debe contener de forma general un Plan de Contingencia (también denominado Plan de Desastre)?

a) Plan de viabilidad, procedimientos de emergencia ante fallos, procedimientos de traslado a instalación alternativa y plan de retorno a instalación primaria

b) Procedimientos de actuación en caso de desastre, plan de copias de seguridad o de almacenamiento/recuperación de información, procedimientos de traslado a instalación alternativa y plan de retorno a instalación primaria

c) Análisis de riesgos informáticos, plan de viabilidad, procedimientos de activación en caso de desastre, plan de almacenamiento/recuperación de información, procedimientos de traslado a instalación alternativa y plan de retorno a instalación primaria

d) Plan de activación de emergencia, procedimientos de emergencia ante fallos y procedimientos de traslado a instalación alternativa

48. A la máxima cantidad de datos que se pueden perder en caso de desastre se les denomina:

a) SDO

b) RPO

c) RTO

d) MTBF

49. El RTO debe ser:

a) superior al MTD

b) independiente al valor del MTD (no importa su relación con el MTD)

c) derterminado por negocio

d) inferior al MTD

50. La medida que tiene relación con el Plan de Continuidad de Negocio en el ENS es la:

a) [op.exp.3]

b) [op.cont.2]

c) [op.cont.11]

d) [mp.fi.3]

51. ¿Qué tipo de centro de respaldo ante desastres ofrece la respuesta más inmediata?

a) Hot site

b) Warm site

c) Instant site

d) Cold site

52. Un local para el procesamiento de la información que dispone de energía eléctrica suficiente, refrigeración y suelo técnico, paneles, puertas, etc. se denomina en el argot de la Continuidad de Negocio:

a) Un "cold-Site" o sitio en frío

b) Un "warm-Site" o sitio tibio

c) Un "Hot-Site" o sitio en caliente

d) Un CPD duplicado "Dupplicate Processing Site"

53. Un plan de continuidad:

a) prepara la respuesta a incidentes y minimiza el impacto de las interrupciones

b) mantiene el nivel de servicio de los sistemas

c) previene de posibles interrupciones en los sistemas

d) prepara la respuesta a incidentes y postpone las interrupciones

54. Teniendo en cuenta que RPO es recoverypoint objective y RTO es recovery time, indique la opción falsa:

a) RPO especifica el intervalo de tiempo entre dos copias de seguridad.

b) El periodo de retención de las copias de seguridad vienen definidos por el RTO.

c) RTO influirá en el tipo de dispositivo donde se realizará la copia de seguridad.

d) En un "full backup" la recuperación se realizará con un RTO menor y una menor cantidad de cintas que si fuera "incremental backup".

55. ¿Qué misión tiene un Plan de Continuidad del Negocio en las organizaciones?

a) Recuperar totalmente la capacidad de operación

b) Recuperar la capacidad de operación de servicios críticos

c) Mejorar la capacidad de operación inicial

d) Restaurar parcialmente la capacidad de operación

56. El plan de continuidad forma parte de las medidas del ENS dentro del:

a) Medidas de protección

b) Marco operacional

c) Marco organizativo

d) Ninguna de las anteriores es cierta

57. ¿Cuál es la mejor medida para lograr efectividad en la continuidad del negocio?

a) Una herramienta de Gestión de incidencias

b) Realiación de revisiones y auditorías períodicas

c) Concienciación de la plantilla

d) Formación a toda la plantilla sobre todos los servicios críticos

58. ¿Cúal no es un objetivo en una prueba de continuidad de negocio?

a) Verificar el RTO para sistemas críticos

b) Verificar la aplicabilidad y suficiencia de la documentación

c) Verificar que el ambiente de contingencia funciona adecuadamente

d) Verificar el impacto en los sistemas críticos

59. El análisis de impacto en el negocio, dentro del plan de continuidad, se realiza:

a) El análisis del impacto de negocio no entra dentro del plan de Continuidad.

b) En las primeras fases del Plan.

c) Al final del plan.

d) No es necesario realizarlo.

60. ¿Cuál de los siguientes tipos de backup es más eficiente en términos de espacio?

a) Backup completo

b) Backup incremental

c) Backup diferencial

d) Backup persistente

61. Ordene las fases propuestas por el INCIBE para la continuidad del negocio:

a) alcance, analisis, estrategia, respuesta, pruebas y mantenimiento, concienciación

b) analisis, estrategia, táctica, operaciones, pruebas y mantenimiento, formación

c) alcance, analisis, estrategia, operaciones, pruebas y mantenimiento, evaluación

d) alcance, analisis, estrategia, respuesta, pruebas y mantenimiento, evaluación

62. El MTD es:

a) El tiempo máximo que se acepta que esté el negocio no operativo.

b) La cantidad de perdida de dato durante un desastre que la empresa considera tolerable.

c) El Tiempo máximo tolerable de caída.

d) A y C son correctas.

63. Indicar cuál de los siguientes no es un apartado contemplado por los criterios SNC del CSAE para elaborar un plan de contingencias:

a) Papeles y responsabilidades de los distintos actores

b) Planificación de recursos cuando se opera en situación de contingencia

c) Criterios para el retorno a explotación normal

d) Todos los anteriores son válidos

64. Indique la sentencia correcta respecto al análisis del factor dolor (Pain Value Analysis), es una técnica:

a) Para ayudar a identificar el impacto en el negocio de uno o más problemas.

b) Para calcular el límite máximo de usuarios que el sistema es capaz de gestionar, teniendo en cuenta la capacidad del hardware y el número de peticiones de cada usuario.

c) Para la asignación de prioridades a diferentes actividades, dice que el 80% del valor de una actividad es generado por el 20% del esfuerzo.

d) Acuñada en los años 80, cuya finalidad era calcular la capacidad física de los usuarios del sistema informático.

65. En el ámbito de la continuidad de negocio, la "ventana de interrupción" se define como:

a) La cantidad de tiempo permitida para la recuperación de un recurso o función de negocio después de que ocurre un desastre.

b) El tiempo que una organización puede esperar desde el punto de fallo hasta la restauración de los servicios o aplicaciones críticas.

c) Se determina en función de la pérdida de datos aceptable en caso de interrupción de las operaciones.

d) Indica el punto más alejado en el tiempo en el que es aceptable recuperar los datos.

66. Un sitio caliente de respaldo se caracteriza por:

a) Altos costes de implementación y mantenimiento

b) Un tiempo reducido de recuperación

c) Un coste reducido de preparación ante desastres

d) La A y la B

67. La organización debe establecer planes de continuidad de negocio que deben contener (señale la errónea):

a) Un proceso que active la prevención ante incidentes

b) Cómo comunicar los incidentes a empleados, familiares, partes interesadas o stakeholders, servicios de emergencia…

c) Cómo continuar el servicio dentro de los periodos establecidos

d) Cómo se dará respuesta del incidente a los medios de comunicación

68. Un parámetro manejado para definir la recuperación de un sistema de información ante un impacto es:

a) Recovery Time Objective.

b) Recovery Plan Objective.

c) Business Recovery Plan.

d) -

69. Un plan de contingencia es una herramienta para emplear en la gestión de las Tecnologías de la Información y las Comunicaciones y aporta una serie de reglas o medidas que proporcionan una garantía de continuidad del negocio y de los procesos de una organización. ¿Cuáles de las siguientes medidas NO se contemplan en la definición de este tipo de planes?

a) Técnicas: Extintores contra incendios, detectores de humo, salidas de emergencia, equipos informáticos de respaldo.

b) Humanas: Formación de actuación ante incendios, designación de responsables de las salas, asignación de roles y responsabilidades para la copia de respaldo.

c) Organizativas: Seguro de incendios, precontrato de alquiler de equipos informáticos y ubicación alternativa, procedimiento de copia de respaldo, procedimiento de actuación ante un incendio, contratación de servicios de auditorías de riesgos laborales.

d) Comunicativas. Se debe comunicar el plan a todos los actores implicados en su ejecución, y a todos los usuarios de los servicios de TI.

70. La realización de simulacros para evuar la capacidad de respuesta ante interrupciones se realiza:

a) en el Plan de Recuperación de Desastres

b) en el plan de Contingencia

c) en el plan de continuidad

d) ninguno de los anteriores

71. Los Sistemas de Gestión de la Continuidad del Negocio (SGCN):

a) utilizan el ciclo Deming

b) utilizan la matriz RACI

c) Ambos dos

d) Ninguno de los anteriores

72. Según la norma ISO/IEC 27031:2011, el conjunto de procedimientos documentados que guían a las organizaciones para responder, recuperar, reiniciar, y restaurar hasta un nivel predefinido de operación después de una disrupción se llama:

a) Plan de Contingencia.

b) Plan de Continuidad del Negocio.

c) Plan de Recuperación ante Desastres.

d) Plan de Respuesta de Emergencia.

73. ¿Cuál es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada aunque el nivel de servicio no sea el óptimo?

a) ROL (Revised Operating Level).

b) RPO (Recovery Point Objective).

c) MTO (Maximum Tolerable Downtime).

d) RTO (Recovery Time Objective).

74. ¿Cuál de las respuestas siguientes es CORRECTA?:

a) El Plan de Continuidad de Negocio engloba el Plan de Continuidad TIC y el Plan de Recuperación ante Desastres.

b) Un Plan de Continuidad de Negocio puede no tener Plan de Recuperación ante Desastres.

c) Un Plan de Continuidad TIC puede no tener Plan de Recuperación ante Desastres.

d) Un Plan de Recuperación ante Desastres puede no tener un Plan de Continuidad de Negocio.

75. La fase de organización de Sistema de Gestión de Continuidad del Negocio no contiene:

a) Realización de reuniones con los usuarios finales

b) Organización de la metodología de mejora continua

c) Identificación de riesgos y amenazas, para su posterior análisios

d) Recopilación de toda la información sobre las aplicaciones del proceso

76. En relación con la recuperación de desastres, ¿a qué se refiere el término tolerancia a desastre?

a) Es el nivel de servicios a proveer durante el modo de proceso alterno hasta que se restaure la situación normal.

b) Es la brecha de tiempo en la cual el negocio puede aceptar indisponibilidad de los servicios de Tecnologías de la Información.

c) Es el plan que organiza la reanudación de los procesos de negocio de la organización que se hayan visto afectados por un fallo o incidente.

d) Es el tiempo máximo que la organización puede soportar procesar en modo alterno.

77. Al planificar el Sistemas de Gestión de la Continuidad del Negocio (SGCN), no debe:

a) Definir sus objetivos de forma clara, así como los relativos a la continuidad de negocio

b) Establecer factores y fuentes internas y externas que provocan riesgos

c) Establecer la probabilidad e impacto de los riesgos

d) Definir la conformidad del dirección estratégica del negocio

78. La fase de planificación de un SGCN abarca:

a) alineación con objetivos y documentación, entre otros

b) la obligatoriedad de la mejora continua

c) el establecimiento de indicadores para los procesos

d) la revisión de la dirección

79. Hacer una previsión de procedimientos de recuperación se debe contemplar en:

a) Plan de Contingencias

b) Control de accesos a bases de datos

c) Mantenimiento y diseño de aplicaciones

d) Ninguna de las anteriores respuestas es correcta

80. Seleccione cuál de los siguientes no es un componente principal de un Sistemas de Gestión de la Continuidad del Negocio (SGCN):

a) implantación

b) planificación

c) mejora continua

d) formación

81. En el ámbito de la continuidad de negocio una operación clasificada como crítica:

a) No puede ser reemplazada por una operación manual.

b) La tolerancia a la interrupción es muy baja.

c) El costo de interrupción es muy alto.

d) Todas las anteriores.

82. En relación a la replicación remota, indica cuál de las siguientes afirmaciones es INCORRECTA:

a) La replicación síncrona proporciona un RPO muy cercano a cero.

b) La replicación síncrona requiere un ancho de banda mayor que la replicación asíncrona.

c) Con replicación asíncrona puede haber pérdida de datos.

d) La replicación asíncrona es más dependiente de la latencia de la red que la replicación síncrona.

83. En base a la estrategia de continuidad, si tenemos un sistema A con una MTD de 123, RPO 8, ROL 50%; que utiliza los sistemas B y C y los RTO de B y C son 66 y 72 respectivamente y ROL de 70%, cuál sería la mejor opción:

a) Debemos asegurarnos que el RPO de B es 66
b) Debemos reducir el RPO de A a 8
c) Debemos reducir el RTO de C a 72
d) Debemos aumentar ROL de B al 80%

84. En el ámbito de la continuidad de negocio, el Punto de Recuperación Objetivo o "Recovery Point Objective RPO":

a) Determina la frecuencia de las copias de respaldo.
b) Indica el punto más alejado en el tiempo en el que es aceptable recuperar los datos.
c) Es la cantidad de tiempo permitida para la recuperación de un recurso o función de negocio después de que ocurre un desastre.
d) A y B.

85. En un BIA, ¿qué actividad se realiza?

a) Evaluar la respuesta de la contingencia.
b) Evaluar el cumplimiento de la estrategia.
c) Evaluar el riesgo e impacto de una interrupción.
d) -

86. ¿Es necesario definir un equipo de gestión de crisis en los planes de contingencia?

a) Si es necesario.
b) Unicamente en las empresas relacionadas con la seguridad nacional.
c) No es necesario en ningún caso.
d) Ninguna de las anteriores es cierta.

87. Respecto a la asignación de personal para la recuperación de interrupciones, señale la opción correcta:

a) debe ser aleatoria y obligatoria
b) debe estar planificada y opcional
c) debe estar planificada y obligatoria
d) debe ser aleatoria y opcional

88. ¿Cuál de los siguientes no es un objetivo del plan de contingencias?

a) Minimizar las interrupciones en la operación normal
b) Limitar la extensión de las interrupciones y de los daños que produzcan
c) Analizar daños y estimar costes
d) Posibilitar la vuelta al servicio rápida y sencilla

89. Los Planes de Continuidad TIC deberían incluir:

a) Plan de Confirmación de Negocio.
b) Plan de Cese en el Negocio.
c) Plan de Ampliación en el Negocio.
d) Plan de Recuperación ante Desastres.

90. Indique la respuesta CORRECTA en relación con el Plan de Continuidad de Negocio:

a) El Plan de Continuidad de Negocio engloba al Plan de Continuidad TIC y al Plan de Recuperación ante Desastres.
b) Un Plan de Continuidad de Negocio puede no tener Plan de Recuperación ante Desastres.
c) Un Plan de Recuperación ante Desastres puede no tener un Plan de Continuidad de Negocio.
d) -

91. ¿El plan de contingencia debe incluir un plan de comunicación?

a) No, cuanto menos se conozca más seguro será.

b) Si, es lo más adecuado.

c) Solo en organizaciones con una complejidad organizaiva grande.

d) Ninguna de las anteriores es cierta.

92. ¿Es necesario un plan de mantenimiento del plan de contingencia?

a) Efectivamente es necesario.

b) Solo es necesario en organizaciones con más de 3000 empleados.

c) El plan de mantenimiento es unicamente propio de las etapas de desarrollo.

d) Ninguna de las anteriores es cierta.