PROGRAMA DE AUDITORIA PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO Y DE LA SEGURIDAD DE LA INFORMACIÓN

Objetivo:

Verificar si los pasos seguidos en el desarrollo del plan, así como las actividades, recursos y funciones implicados, han sido objeto de planificación previa, y determinar si el proceso seguido en su elaboración ha sido idóneo para garantizar el resultado de un plan eficaz de cara a la restauración progresiva de los servicios y de los procesos que los sustentan.

Desarrollo de la auditoria bajo el sistema de indagación y comprobación

Cada una de las preguntas formuladas, deben ser debidamente soportadas con la evidencia documental, para esto el auditado deberá soportar mediante evidencia escrita o por otros medios viables la sustentación de las mismas:

A. Preguntas generales para el desarrollo del programa de auditoria:

1. ¿Está debidamente aprobado por la Gerencia, tanto el plan como la política de seguridad de información?
2. ¿Fecha de aprobación y evidencia física de la misma?
3. ¿El plan se elaboró con arreglo a un proyecto documentado y autorizado que se conserva adecuadamente?; Estas preguntas indican la autoridad e importancia que la entidad a través de los directivos conceden al plan, y si está debidamente tratado y guardado.
4. ¿Qué se intenta proteger?
5. ¿Se corresponde con los objetivos del área y estratégicos de la organización?
6. ¿Se han determinado correctamente las amenazas?
7. ¿Mediante cual metodología se establecieron las amenazas?
8. ¿Se han determinado con corrección las vulnerabilidades presentes en la organización?
9. ¿Cuál es el valor de los activos para la organización?
10. ¿Frente a qué se intenta proteger?
11. ¿Cuál es la probabilidad de ataque?
12. ¿En dicho proyecto se consideraron las posibles amenazas sobre los recursos adecuadamente?

13. ¿Se definieron las actividades a realizar para la elaboración del análisis de riesgos e impacto y se designaron a las personas adecuadas para valorarlas?
14. ¿Se han definido las criticidades de las funciones de manera adecuada?
15. ¿Se han indicado contramedidas efectivas que se corresponden con el análisis de la situación realizada?

B. Fase de desarrollo de la estrategia

1. ¿Se han identificado correctamente las necesidades que debe cubrir la estrategia de continuidad de negocio seleccionada?
2. ¿Se han considerado las estrategias alternativas mencionadas en la anterior consideración de la pregunta y su idoneidad para la entidad?
3. ¿El centro elegido para la recuperación es propio o contratado?
4. ¿Es adecuado en función de los objetivos?
5. ¿Se puede utilizar el centro para pruebas?
6. ¿Es utilizado para las necesidades de un tercero en caso de que sea contratado a una compañía externa?
7. ¿Si hay más de una compañía, hay suficiente tiempo de proceso disponible?
8. ¿Existe un documento legal que respalde y refleje lo que realmente se contrató?

C. En el caso de la contratación

1. ¿Hay suficiente tiempo de proceso para nuestras necesidades?
2. ¿Somos puntualmente informados de todos los cambios que se puedan producir dentro de los sistemas tanto de software como de hardware del centro alternativo?
3. ¿Se ha especificado el costo de contratación?
4. ¿La distancia con el centro de desarrollo de nuestras actividades es lo suficientemente cercana como para permitir una fácil recuperación de las operaciones?
5. ¿Se encuentra dicho centro a una distancia que lo cubra de desastres naturales que puedan afectar al centro donde se desarrolla el trabajo habitualmente?
6. ¿El proveedor dispone de un equipo de atención que permita acceder de una manera eficaz a los servicios propios que ofrecen?
7. ¿Dan soporte alternativo de mantenimiento o ingeniería?
8. ¿La disponibilidad de los servicios es absoluta?
9. ¿Qué medidas de seguridad existen en el centro?
10. ¿Qué espacio adicional de oficinas hay disponible?

11. ¿Se proveerán técnicos de sistemas u operadores?
12. ¿Qué comunicaciones hay disponibles?
13. ¿Qué pruebas del plan pueden hacerse?
14. ¿Se suministra espacio de almacenamiento?
15. ¿Cuál es el procedimiento de petición del servicio, funciona correctamente?
16. ¿Durante cuánto tiempo se pueden usar las instalaciones?
17. ¿Es suficiente?
18. ¿Qué procedimiento se seguirá para atender más de una petición simultánea?
19. ¿Se han determinado las responsabilidades en cada fase de traslación del plan de contingencia al lugar de recuperación?,
20. ¿Se han determinado los precios específicos de los servicios?

D. Fase de la normalidad

1. ¿Están contemplados y definidos los posibles sucesos que pudieran ocurrir y las situaciones, diferentes de la normalidad, que se pudiesen dar?
2. ¿Se determina con precisión el procedimiento a seguir antes de declarar la situación de emergencia, así como las personas que, en su caso, deben efectuar dicha declaración?
3. ¿Están contempladas las actuaciones de respuesta para recuperar la actividad y definidas según un orden de prioridades?
4. ¿Se asignan responsabilidades en su ejecución (actuaciones), que son conocidas por los empleados designados y éstos cuentan con la formación y entrenamiento necesarios para caso de siniestro?
5. ¿Se han identificado claramente y tenido en cuenta los componentes de un procedimiento de respuesta ante una emergencia?
6. ¿Existe un equipo o comité de dirección de la reanudación y un responsable del mismo para dirigir y coordinar las distintas actividades durante la contingencia o desastre?
7. ¿Del equipo de reanudación o recuperación y de cualquier otro previsto en el plan, se han definido sus componentes y funciones, así como los procedimientos y actividades que cada equipo ha de realizar para cada uno de los niveles de siniestro contemplados, incluida la reconstrucción del centro de proceso de datos si fuese necesario?
8. ¿Para la reanudación del funcionamiento de las aplicaciones críticas, están definidas las necesidades de hardware, software y comunicaciones?
9. ¿Están definidas unas normas sobre copias de seguridad de ficheros, que están aprobadas, actualizadas y se cumplen?

10. ¿Están definidos unos procedimientos de obtención de copias de forma controlada y éstas se renuevan en los períodos establecidos?
11. ¿Existe un inventario detallado de las copias de seguridad necesarias para la recuperación de los ficheros de las aplicaciones críticas y están definidas sus características?
12. ¿La documentación correspondiente a las aplicaciones críticas existe y al igual que las copias de seguridad de los ficheros se conservan en otro edificio?
13. ¿Están definidas las condiciones de custodia, acceso y uso de las copias de seguridad?
14. ¿Está detallada la ubicación del centro alternativo de respaldo de proceso de datos, así como la configuración del mismo?
15. ¿En relación con dicho centro, también se contemplan los requerimientos de hardware, software de explotación, ficheros, acuerdos con los proveedores, así como la inclusión del software de seguridad de dicha instalación?
16. ¿Se ha tenido en cuenta el área de comunicaciones, las redes corporativas y las redes de área local?
17. ¿De los ordenadores personales que tienen información crítica existen procedimientos de recuperación específicos?
18. ¿Están definidos unos procedimientos manuales de respaldo?
19. ¿Se han desarrollado procedimientos detallados de respuesta ante emergencias?
20. ¿Se han identificado todas las necesidades de dirección y control, así como sus procedimientos?
21. ¿Se ha creado un equipo para el salvado y restauración y definido una estrategia para la actividad inicial in situ?
22. ¿Se puede deducir de la experiencia de los siniestros acontecidos en el pasado alguna conclusión que no se corresponda con el estado actual del plan?
23. ¿Han cambiado las estrategias y por tanto es necesario reorientar el plan y por eso no es posible unas el desarrollo de la fase de revisión de esta?
24. ¿Se han desarrollado y probado los procedimientos para asignación de prioridades en la respuesta ante emergencias?

E. Mantenimiento y pruebas

1. ¿Están designadas las personas responsables del mantenimiento del plan?
2. ¿Está definido un calendario de actualizaciones para las diferentes funciones?

3. ¿Se cumplen los plazos establecidos para la revisión y actualización del plan?
4. ¿Ante cambios significativos en los recursos de la empresa o en el entorno en el que se encuentra, se realiza una actualización del plan?
5. ¿Las actualizaciones realizadas se registran?
6. ¿Se han planificado las pruebas del plan y establecido plazos, motivos y responsable de las mismas?
7. ¿Las pruebas se realizan puntualmente dejando constancia documental y se corrigen los fallos detectados?
8. ¿Existe un desarrollo de programas de revisiones del plan?
9. Si es así: ¿Siguen siendo críticas las funcionalidades revisadas?
10. ¿Se sigue revisando si cumplen con los umbrales de recuperación establecidos?
11. ¿Se han incluido en las revisiones nuevas funcionalidades que antes no eran críticas?
12. ¿Se han llevado a cabo entrenamientos para la formación del personal y que puedan desarrollar las revisiones o pruebas?
13. ¿Están definidos los objetivos de los entrenamientos?
14. Si es así. ¿Se refleja su efectividad en las experiencias o siniestros del plan acontecidos anteriormente?
15. ¿Se ha establecido un programa de pruebas? Si es así, cubre los siguientes puntos:
16. ¿Tiene un enfoque lógico y estructurado?
17. ¿Pone en peligro la continuidad de las operaciones?
18. ¿Es práctica y apropiada a la organización?, ¿Es limitada y eficaz en el coste?, ¿Asegura un alto nivel de confianza en la capacidad de recuperación?
19. ¿Tiene un conjunto de directrices adecuado?
20. ¿Establece una periodicidad realista?
21. ¿Tiene una asignación adecuada de recursos?
22. ¿Existe una definición adecuada de las necesidades de las pruebas?
23. Si es así: ¿Existe una identificación de tipos de pruebas?, (simulaciones, pruebas modulares, pruebas funcionales, pruebas anunciadas, pruebas por sorpresa)
24. ¿Cuál de ellas aporta éxitos o ventajas?
25. ¿Se han creado escenarios realistas que se corresponden con incidentes probables?
26. Si es así: ¿Se ha entrenado a los miembros del equipo de recuperación ante situaciones nuevas?
27. ¿Se han probado las comunicaciones, métodos de documentación y registros del centro de control?
28. ¿Existe una serie de criterios de evaluación objetivos de los resultados de las pruebas?

29. ¿Se ha seleccionado la metodología de pruebas más adecuada?
30. ¿Se han definido con certeza los objetivos de las pruebas?
31. ¿Se ha especificado un plan de controles de las pruebas y un método de información de los resultados a la dirección?
32. ¿Qué acciones correctoras y de retroalimentación son resultado de las pruebas, y si son adecuadas?
33. ¿Existen procedimientos adecuados para el control de cambios?