ANEXO TÉCNICO 4
SOLUCIÓN DE BACKUPS

OBJETIVOS

El servicio proporcionado le permitirá a la Escuela Superior de Administración Publica ESAP tener una plataforma de Backup y esquema de recuperación de desastres que le de la capa inicial para establecer un esquema de continuidad del negocio,

ALCANCE

Se llevará a cabo la creación de políticas de Backups requeridas por la Escuela Superior de Administración Publica, al igual que la implementación de los servicios de la herramienta de Backup de Microsoft System Center 2016 Data Protection Manager, con esto se requiere la generación de los procesos requeridos para que la Escuela Superior de Administración Publica ESAP, pueda iniciar con del desarrollo de un plan de continuidad del negocio.

REQUERIMIENTOS

1. La solución requerida por la Escuela Superior de Administración Publica ESAP considera los siguientes aspectos a desarrollar :
    a. Análisis de riesgos de procesos del negocio.
    b. En esta fase se realizará la identificación y evaluación de riesgos que pueden generar una afectación en la operación de los procesos críticos de la ESAP, considerando:
        i. Identificar los riesgos que pueden provocar una afectación en la operación de los procesos críticos, con base en las amenazas y vulnerabilidades identificadas.
        ii. Calificar los riesgos identificados con base en su probabilidad de ocurrencia e impacto.
        iii. Definir un mapa de riesgos.
        iv. Determinar las medidas preventivas, efectivas y correctivas a implementar para mitigar los riesgos operacionales identificados de conformidad con el apetito por el riesgo de la Secretaría.
        v. Determinar los escenarios de riesgo.
2. Presentar una fase en que se deberá realizar un análisis de brechas de la Estrategia de continuidad actual contra los resultados del Análisis de Impacto al Negocio (BIA) y la Evaluación de Riesgos (RA), considerando:
    a. Determinar si la Estrategia de Continuidad actual considera los escenarios de interrupción identificados durante la fase de Evaluación de Riesgos (RA)
    b. Determinar si los requerimientos de personal, registros vitales, tiempos de recuperación y puntos de recuperación de los procesos críticos identificados durante la fase de Análisis de Impacto al Negocio (BIA) están cubiertos por la Estrategia de

Continuidad actual.

c. Determinar si la capacidad de continuidad del negocio de los proveedores críticos incluidos en la Estrategia actual cumplen con los requerimientos identificados durante la fase de Análisis de Impacto al Negocio (BIA).

d. Determinar las políticas, procedimientos, roles y responsabilidades que deben ser implementados y formalizados en la Secretaría para la gestión y para la implementación de un Plan de Continuidad del Negocio que responda ante los escenarios de riesgo identificados.

3. Documento de Informe de Evaluación de Riesgos de Procesos de Negocio que contenga como mínimo:

   a. Objetivo.

   b. Alcance.

   c. Identificación de riesgos de procesos de negocio.

   d. Definición de criterios para la evaluación de riesgos.

      i. Impactos, probabilidades.

      ii. Nivel de Riesgo.

   e. Resultados de la evaluación de los riesgos de procesos de negocio.

      i. Mapa de riesgos.

      ii. Definición de acciones propuestas para el tratamiento de los riesgos identificados.

      iii. Definición de escenarios de riesgo.

4. Documento con el análisis de las brechas de la Estrategia de Continuidad actual de la Secretaría contra los resultados del Análisis de Impacto al Negocio (BIA) y la Evaluación de Riesgos (RA), que incluya:

   a. Objetivo.

   b. Alcance.

   c. Análisis de los requerimientos de continuidad identificados en el BIA contra la Estrategia de Continuidad Actual para determinar los requerimientos que deben de ser imple mentados:

      i. • Procesos críticos.

      ii. • Personal crítico y suplentes.

      iii. • Registros vitales.

iv. • Productos y servicios de proveedores externos, organismos y entidades regulatorias.

v. • Tiempos de Recuperación.

vi. • Puntos de Recuperación.

d. Análisis de las políticas, procedimientos, roles y responsabilidades requeridos para la gestión de la Continuidad del Negocio contra los componentes de la Estrategia de Continuidad actual, considerando:

i. • Políticas de Continuidad del Negocio.

ii. • Roles y responsabilidades.

iii. • Árboles de llamadas.

iv. • Plan de Continuidad del Negocio (BCP).

v. • Procesos para la Gestión de Continuidad del Negocio (SGCN)

vi. ▪ Supervisión, medición y evaluación.

vii. ▪ Capacitación y concientización.

viii. ▪ Pruebas.

ix. ▪ Actualización de documentos.

5. Realizar el levantamiento de información de los servicios core de la Escuela de Administración Publica la cual cuente con la siguiente información:
    a. Listado de los principales servicios Core prestados por el departamento de TI
    b. Plan actual de Backups
    c. Procesos actuales de Backup y restauración de los servicios e información
6. Realizar reporte de estado actual de los servicios de Backup y recuperación de la información.
7. Realizar un reporte de los factores o eventos que puedan interrumpir los servicios que provee el departamento de TI.
8. Realizar reporte del estado actual de los procesos de continuidad del negocio.
9. Establecer las políticas de Backup requeridas para la infraestructura tecnológica y los servicios de Informacion sobre el siguiente esquema:
    a. Diario
    b. Semanal
    c. Mensual

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co

d. Anual

10. Realizar el diseño y arquitectura para la implementación de la herramienta de Backup de Microsoft System Center 2016 Data Protection Manager
11. Establecer las estrategias adecuadas para realizar los Backups de:
    a. Aplicaciones
    b. Servidores de archivos
    c. Servicios Virtualizados
12. Realizar la implementación de la herramienta de Microsoft System Center 2016 Data Protection Manager.
13. Realizar la configuración para realizar los Backup de forma adecuada de los servicios de virtualización bajo la herramienta de Microsoft System Center 2016 Data Protection Manager.
14. Desarrollar un plan de capacitación enfocado a los administradores de la herramienta de Backup de Microsoft System Center 2016 Data Protection Manager.
15. Realizar un esquema de capacitación que se componga de un total de 20 horas enfocado a los administradores de la herramienta
16. Realizar un plan de capacitación o adopción de los procesos de continuidad del negocio enfocado al área de TI el cual se componga de un total de 20 horas de capacitación.

BOGOTÁ
Calle 93B No. 13 – 44 piso 2
PBX: (+571) 746 6000

MANIZALES
Cra. 24 No. 53ª – 26 – Arboleda Alta
PBX: (+576) 886 1212

www.infotic.co