En esta ocasión mostramos un nuevo checklist genérico de la serie que hemos estado publicando, en esta ocasión mostramos un checklist centrado en plataformas de Backup centradas en entornos virtuales.

La capacidad de Protección y Recuperación de datos describe los procesos y herramientas utilizados de las copias de seguridad, almacenamiento y recuperación de datos y aplicaciones. Conforme aumenta la cantidad de información disponible y los almacenes de datos, las organizaciones se ven cada vez más presionadas para proteger esta información y disponer de procesos de recuperación económicos y eficientes para situaciones de emergencia.

La funcionalidad de este checklist es garantizar que todo entorno disponga de un medio de copias o procesos de copias de seguridad, así como el método para su recuperación en caso de desastre, perdida de datos o eliminación de los mismos por causas propias o ajenas. Para ello se establece un documento que contendrá los distintos procedimientos o procesos de copias de seguridad y restauración. El objetivo es asegurar la integridad de los datos.

En este punto el cliente deberá de facilitar un documento resultante que deberá de disponer de los siguientes elementos:

- Copias de Seguridad
- Política de copias a aplicar (diaria/incremental/total/semanal/mensual).
- Perfiles
- Ficheros a copiar.
- Volumen de copias a realizar (GB/TB).
- Estructura.
- Arquitectura del sistema de copias.
- Elementos de copia.
- Hardware utilizado
- Fabricante
- Modelo
- Software
- Fabricante
- Versión
- Restauración de copias.
- Proceso y Plan de restauración.
- Procedimiento de restauración.

Los puntos más importantes a tener en cuenta en un proceso de copias y restauración de datos, en este caso el cliente deberá de facilitar la siguiente información:

- Confidencialidad. El sistema contiene información que requiere protección contra la divulgación no autorizada. Por ejemplo, datos que se van a difundir en un momento determinado (como, información parcial de informes), información personal e información comercial patentada.
- Integridad. El sistema contiene información que debe protegerse de modificaciones no autorizadas, imprevistas o accidentales. Por ejemplo, información de censos, indicadores económicos o sistemas de transacciones financieras.
- Disponibilidad. El sistema contiene información o proporciona servicios que deben estar disponibles puntualmente para satisfacer requisitos o evitar pérdidas importantes. Por ejemplo, sistemas esenciales de seguridad, protección de la vida y predicción de huracanes.

***Como siempre cualquier mejora será siempre bienvenida.**