ESTADO LIBRE ASOCIADO DE
PUERTO RICO
DEPARTAMENTO DE EDUCACIÓN

Procedimiento de Resguardo y Recuperación Mediante *Tivoli Storage Manager*

Recomendado por:

Ing. Maribel Picó Piereschi
Oficial Principal de Informática

Fecha: 5-8-2015

Aprobado por:

Prof. Rafael Román Meléndez
Secretario

Fecha: 15/6/15

Tabla de contenido

Resumen ejecutivo

Este documento define el procedimiento de resguardo y recuperación de los datos del Departamento de Educación (DE) del Estado Libre Asociado de Puerto Rico para los servidores de la plataforma de IBM y los sistemas operativos Windows 2000 / 2003 / 2008 / 2012 con la aplicación de *Tivoli Storage Manager* (TSM). En el mismo se describen los objetivos, funciones, políticas y procedimientos relacionados a las diversas alternativas de resguardo y recuperación de datos. El DE ejecuta el procedimiento de resguardo con la plataforma de TSM para asegurar la protección de los datos de los sistemas de la institución. Para la confección de éste documento se utilizaron como base las mejores prácticas en la industria para este proceso y referencia de experiencias de consultores de IBM y *Truenorth Corporation.*

Alcance

El procedimiento de resguardo considera los datos y sistemas clasificados críticos o datos corporativos que se resguardan con la herramienta TSM. Este no considera políticas y procedimientos para resguardo, restauración y recuperación de datos de los usuarios en computadoras personales. Este no incluye procesos de "*backup / restore*" para las estaciones de trabajo de los usuarios y de servidores que no están definidos en la plataforma de resguardo (*backup)* de TSM. Este procedimiento no constituye un Plan de Desastre para los sistemas del DE.

Objetivo

El proceso de resguardo de los datos, transacciones y sistemas de información es un estándar en los centros de cómputos, para aplicaciones críticas en la operación de las industrias. Por tal razón, el DE establece por medio de este documento una estrategia de resguardo con los siguientes objetivos:

- Contar con la política y procedimiento de resguardo, restauración y recuperación de datos mediante la herramienta TSM.
- Mantener actualizada la información de la infraestructura del DE (red, sistemas operativos, servidores, etc.).
- Automatizar e implementar el proceso de resguardo.

Limitaciones

Actualmente el DE no cuenta con un centro alterno equipado con las especificaciones necesarias para recuperar los datos y sistemas. Sin embargo, está en el proceso de evaluar alternativas, tales como:

- Identificar instalaciones del DE para preparar el centro alterno.
- Contratar los servicios de un centro alterno a una empresa establecida en o fuera de Puerto Rico.

Aspectos generales

Las siguientes tareas son necesarias para definir los datos que se van a resguardar y los recursos necesarios para la operación:

- Clasificar, almacenar, restaurar y recuperar datos.
- Desarrollar las políticas y procedimientos para almacenar, restaurar y recuperar datos.

El proceso de monitorear los datos y los recursos incluye:

- Monitorear los recursos de informática (sistema y base de datos) para verificar la capacidad y la disponibilidad, la configuración, y para medir el rendimiento.
- Monitorear los recursos de almacenamiento de los datos para asegurar que funcionan adecuadamente y que son los apropiados según las necesidades del DE.
- Realizar estudios de capacidad para determinar necesidades futuras de acuerdo con el Plan de Tecnología y de tendencias actuales.

El mantenimiento de los datos y de los recursos requiere:

- Solicitar aprobación para cualquier cambio que afecte el Proceso de Resguardo establecido, por medio de la Solicitud de Cambio (Anejo).
- Mantener los recursos necesarios para garantizar la disponibilidad y el rendimiento de los sistemas de información
- Asegurar que los datos se almacenan de acuerdo con las políticas establecidas de seguridad y las mejores prácticas para este proceso.

Definiciones

Resguardo (*Backup)*-Es un proceso en el que periódicamente se copian los datos y la información de un medio o dispositivo electrónico (típicamente disco duro) a un segundo medio o dispositivo. El propósito es recuperar los datos, en caso necesario, en el tiempo establecido.

El segundo medio, típicamente cartuchos de cintas magnéticas asignadas a una librería de *backup*, aplica al resguardo de los datos de servidores manejado por la aplicación de TSM.

Dependiendo de los requisitos de almacenamiento de información o datos, ésta puede ser guardada por largos periodo de tiempo, en algunas ocasiones de por vida. Este proceso se conoce como archivo de datos (*Data Archiving*). El proceso de almacenamiento de estos es especial y es necesario que se informe de esta necesidad para considerarla en el proceso de planificación de capacidad del espacio en su almacenamiento externo.

Restauración de datos (*Restore*) - Proceso en el que se restauran datos o información, sea de un archivo o de varios, en un segundo servidor o equipo de almacenaje. Los datos se resguardan en el disco duro del servidor identificado o en el equipo de almacenaje correspondiente.

Recuperación de datos (*Data Recovery*) - Proceso en el que se restauran todos los datos a su estado original antes de un evento o a causa de un desastre que ocasiona pérdida completa de los datos o la corrupción de los mismos. Los desastres pueden ser causados por terremotos, huracanes, inundaciones, colapso de un servidor, entre otras razones. El director del Centro de Cómputos y otro personal técnico de OSIATD evaluarán los eventos para determinar cuándo una interrupción de un servicio se considera o se declara desastre.

Proceso de resguardos - Este se enfoca en los aspectos de operación y mantenimiento. Este define, monitorea y mantiene los datos y los recursos necesarios para la operación de uno o de varios sistemas de información.

Función y responsabilidades dentro del proceso de resguardo

El proceso de resguardo es una operación crítica que se ejecuta diariamente en todos los centros de cómputos. Esta sección describe las funciones y responsabilidades de este grupo de trabajo. Algunas de estas funciones son parte de las tareas diarias del proceso, mientras que otras son requeridas en el proceso completo. Dependiendo del tamaño y la complejidad de la organización, un individuo puede realizar más de una función. Sin embargo, debe haber un solo responsable por el proceso, quien se designará como administrador de resguardo y estará a cargo de atender y resolver cualquier situación que se presente. A continuación, las funciones y responsabilidades específicas:

Rol	Responsabilidades
Administrador de resguardo	El administrador de resguardo es el dueño del proceso completo con responsabilidad total del mismo. Es responsable por el diseño y la reestructuración del mismo, así como de las mejoras que afectan todo el proceso. Este es responsable por las otras funciones que cubren todo el proceso y los individuos que las ejecutan. Estas actividades pueden tomar de un 25% a un 75% de su tiempo. El administrador de resguardo es responsable de las siguientes tareas: • Determinar las estrategias de resguardo, restauración y recuperación de datos. • Asegurar que los procedimientos de resguardo, restauración y recuperación se cumplan y que los mismos son adecuados. • Asegurar que la documentación sea debidamente completada. • Asegurar que el equipo de trabajo tiene el conocimiento y las herramientas adecuadas para ejecutar su trabajo. • Procesar las peticiones de resguardo y restauración • Asegurar que los procedimientos de resguardo cumplen con las reglamentaciones y regulaciones relacionadas a la información del Departamento de Educación. • Proveer y controlar el uso limitado de los medios de resguardo (cintas, cartuchos, etc.). • Auditar los resguardos para asegurar consistencia de los datos lógicos y físicos. • Buscar y cargar el medio para el resguardo y la restauración de datos. • Asegurar la instalación y remoción del medio para el resguardo y la restauración de los datos. • Proveer y controlar el medio para ambientes de prueba. • Proveer y controlar el medio para ambientes de producción. • Mantener inventario de los medios y notificar con suficiente anticipación la necesidad de nuevos medios. • Manejar el medio según las recomendaciones del manufacturero.

Rol	Responsabilidades
Operador del centro de cómputos	El operador del centro de cómputos mantiene las cintas de resguardo y es responsable de: • Asegurar que el transporte del medio fuera del Departamento de Educación cumpla con las políticas de retención y rotación. • Mantener un registro de los resguardos y del cartucho de resguardo depositado fuera y recibido al Departamento de Educación.

Clasificación de los datos

La clasificación de los datos se define de acuerdo con la importancia e impacto para la continuidad de las operaciones del DE, por requerimientos específicos de reglamentación y leyes, aspectos fiscales y económicos e imagen pública, entre otros.

Categorías para clasificación de los datos

Categoría de los Datos	Descripción
Confidencial	Datos críticos para el DE cuyo contenido es confidencial.
Crítica	Datos de gran importancia cuya pérdida puede causar un impacto negativo a las finanzas o imagen pública, repercusiones de índole legal, tales como demandas y querellas, entre otras. En esta categoría se encuentran los datos relacionados a nómina, recursos humanos, documentos legales, etc.
Prioridad alta	Datos que, en menor grado, su pérdida afecta la operación de todo el DE. Ejemplo de esto es: • Correo electrónico • Página cibernética Datos que impactan la operación de un programa u oficina clave. Ejemplos de esto son: • Oficina del Secretario • División Legal, entre otros. Datos que pueden alterar los compromisos y promesas del DE.
Prioridad media	Datos que son pertinentes o que afectan la operación de un programa u Oficina, cuya pérdida o falta de acceso puede afectar los servicios provistos, pero no la operación total del DE. La recuperación de estos datos requiere de una inversión de tiempo y recursos mínimos.

Prioridad baja	Datos de poco valor que, en caso de pérdida, no afectan la operación del DE o afectan la operación directa de uno o pocos empleados. En esta clasificación, para propósitos de este procedimiento, se encuentran los datos de los usuarios en sus estaciones de trabajo. (*Personal computer* – PC) Nota: Al crear un directorio para un usuario, el administrador debe tomar en consideración la clasificación de los datos del mismo. Dependiendo el nivel o autoridad del usuario, este puede tener acceso a datos críticos que deben protegerse de acuerdo con el procedimiento aquí presentado.
No resguardo	Datos que se almacenan en un directorio para acceso compartido. Estos datos pueden ser localizados y restaurados sin mayores consecuencias. Ejemplo de esto son: • *Drivers* de impresoras, escaners, entre otros. • Distribución de productos como *Microsoft Office, Windows 2000, Service Pack*, etc.

Proceso de resguardo

Método

El resguardo normal de los datos se realiza diariamente. Además, se realiza un resguardo semanal y uno mensual. El resguardo semanal se realiza el último día de la semana y el mensual se lleva a cabo el último día del mes. El cartucho con los datos de cada semana y el mensual se almacenan en una bóveda externa durante un año o más, depende de la política de retención.

Frecuencia

El resguardo diario (incremental) es el proceso de resguardo de los datos que se añaden o se modifican en los sistemas o aplicaciones desde el resguardo del día anterior. El resguardo diario de la base de datos de SQL y *Exchange* es completo y en línea. *(Full backup and online*)

Los resguardos semanales y mensuales son completos (*full*) y de forma *offline*.

El proceso de resguardo se realiza fuera de horas laborables para no afectar las operaciones y los servicios a los usuarios. Para esto se utiliza el sistema o aplicación de TSM.

El dispositivo (cartucho) se almacena en la bóveda del DE y en una bóveda externa, *International Safe Deposit*.

Itinerario (*Schedule*) de resguardos

El administrador de resguardo define el itinerario de los resguardos automáticos. El administrador / operador reemplaza los cartuchos, verifica que el proceso se complete exitosamente y que el contenido del resguardo es confiable. Los resguardos automáticos se ejecutan según el orden identificado en la tabla en Apéndice G, dado que se ejecutan varios itinerarios simultáneamente para completar el proceso en un tiempo razonable. La tabla indica los itinerarios, el método y la frecuencia que aplican a cada uno.

Cuenta administrador

Siguiendo las mejores prácticas, los resguardos se ejecutan con la cuenta creada y asignada solo con este fin y con privilegios de *TSM Administrator*. Debido al nivel de privilegios de esta cuenta, la contraseña (*password*) se cambia mínimo cada 90 días. Esta cuenta está asignada al administrador de resguardo.

Almacenamiento de resguardos

El DE cuenta con una bóveda que cumple con los requisitos necesarios para el almacenamiento de los dispositivos (cartuchos), así como un lugar alterno fuera de las instalaciones del DE, de acuerdo con las mejores prácticas. Esto, por si un desastre afecta la operación del centro de cómputos, se puedan restaurar los sistemas identificados y recuperar los datos en un centro alterno. El administrador debe considerar las proyecciones de crecimiento para definir las necesidades de almacenaje.

El Proceso de Resguardo tiene que considerar las necesidades de incremento de recursos de acuerdo con los comportamientos observados, las tendencias de crecimiento del tamaño de las bases de datos u archivos de datos, y de los servicios ofrecidos. Es importante que el administrador de resguardo esté al tanto de los planes de tecnología e implantación de nuevos sistemas. Con la información identificada, el administrador realizará proyecciones de crecimiento y determinará los recursos necesarios.

Políticas de retención de resguardo

En esta sección se describen las políticas de retención de resguardo del DE. Estas son:

- Para los resguardos diarios y en forma incremental se mantienen las últimas dos versiones de los archivos resguardados. Además, un archivo o directorio que es borrado por el usuario está disponible en TSM por un periodo de 60 días.
- Para los resguardos diarios de las bases de datos de SQL y Exchange se mantiene una cantidad de siete (7) versiones de resguardo.
- Para los resguardos semanales o mensuales, tienen un periodo de retención desde un mes hasta 5 años. El administrador de TSM utiliza la hoja para llevar o mantener registro de los resguardos realizados (Apéndice B).

Manejo de los cartuchos

El manejo de los cartuchos se divide en dos (2) categorías. La primera categoría se refiere a los cartuchos que están en las librerías. La segunda categoría se refiere a los cartuchos que son transportados a la bóveda externa (*Internacional Safe Deposit*).

- Se remueven los cartuchos de la librerías – (LTO-*Copypool* y los cartucho de la base de datos – {*Snapshot y DBBackup*}) y se reemplazan con los cartucho que son categorizados como *scratch*.
- Luego que se remueven los cartuchos de las librerías, el administrador cumplimenta el formulario (Apéndice B) y lo entrega al personal del centro de Cómputo designado para llevarlo a la bóveda externa *(Internacional Safe Deposit).*

Registro de los cartuchos de resguardo

El operador del centro de cómputos utiliza el Formulario de Manejo de Cartuchos y verifica que la información de los cartuchos está correcta, firma el formulario, envía una copia al administrador y luego archiva la copia para futura referencia.

Informes diarios

- Se genera un informe diario del proceso y estatus *(TSM Operations Daily Checklist)* y se envía una copia al supervisor y a otro personal del centro de cómputos, con el objetivo de verificar la consistencia del proceso diario y el estatus del sistema (ver Apéndice C) donde se identifican los trece (13) pasos de los eventos ocurridos durante el proceso diario.

- El sistema TSM genera automáticamente un informe (*Client Backup Results TSM 16 hour Report for* DE-TSM-001-A) que indica si el proceso de resguardo se completó exitosamente. La aplicación de TSM envía este informe, por correo electrónico, al personal identificado. Esta hoja es para verificar que todos los servidores hayan completado el resguardo (Ver Apéndice D).

- Para el proceso de resguardo que no se pueda ejecutar adecuadamente, se genera un informe (TSM *Operations - Troubleshooting Log)* en que se identifican los servidores para el cual el proceso de resguardo falló y el remedio para completar el mismo (ver Apéndice E).

Pruebas de recuperación de datos

Como parte de la estrategia de respaldos en el DE, se llevan a cabo pruebas de los respaldos realizados para validar el proceso. Debido al costo envuelto y la complejidad en realizar las pruebas, estas se realizan en periodos determinados. La prueba de recuperación de datos se realiza en servidores equivalentes en ambientes virtuales.

Como parte de los resultados de las pruebas también se incluyen los resultados de varios procesos de recuperación que se realizan en servidores de producción.

Itinerario para Pruebas de Recuperación de Datos

Para mantener la continuidad de los procesos se realizarán pruebas cada seis (6) meses, durante los meses de junio y diciembre. La fecha específica de la prueba de las aplicaciones críticas, se determinará de acuerdo a los procesos o itinerarios de trabajo durante ese periodo.

Procedimiento para Pruebas de Recuperación de Datos

En coordinación con el usuario / dueño de la aplicación:

1. Determinar los datos que se utilizarán para la prueba de recuperación. La prioridad para realizar estas pruebas son las aplicaciones críticas y para esto se utilizará un conjunto de datos significativos de la misma que determine el usuario / dueño de la aplicación.

2. Preparar las máquinas virtuales (servidores) que se utilizarán para las pruebas de recuperación de datos.

3. Realizar el proceso de recuperación de los datos en los servidores escogidos para pruebas. La recuperación de los datos se hará a un directorio escogido para el servidor en específico.

4. Recopilar los resultados de la corrida de recuperación y el tiempo que tomo el proceso en completar.

5. Referir los resultados al usuario / dueño de la aplicación para que valide los mismos, no más tarde de 1 semana de recibir los mismos. Se utilizará la forma RIVF – Restore Test Validation form (Apendice H).