



BAREMETAL DATA

PROTEGIENDO LOS DATOS "OFFSITE"



Protecting Your Data Off-site Copyright

Traducido con autorización del autor.

© 2006 por BareMetal Data



PRIMERA EDICIÓN: 23 de Agosto, 2006

Todos los derechos reservados.
Ninguna parte de este documento puede ser reproducido o producido de ninguna forma o a través de ningún medio, electrónico o mecánico, incluyendo fotocopiado, grabación o cualquier sistema de almacenaje o recuperación de información sin el permiso escrito por parte del editor, excepto para la inclusión de breves anotaciones en una revisión.

Marcas Registradas

Todos los términos mencionados en este documento que se conocen como marcas registradas o marcas de servicio han sido capitalizadas de manera apropiada. BareMetal Data no puede testificar por la validez de esta información. El uso de un término en el presente documento no debe ser visto como una afectación a la validez de ninguna marca registrada o marca de servicio.

Advertencia y Renuncia de Responsabilidad

Este documento ha sido diseñado para proveer información sobre la protección de los datos al enviarlos fuera de sitio. Se han hecho todos los esfuerzos posibles para hacer este documento tan completo y tan exacto posible, pero no se implica ninguna garantía o capacidad específica.

La información es provista sobre una base implícita. Los autores de este documento no tendrán ni la posibilidad, ni la responsabilidad ante ninguna persona o entidad con respecto a la pérdida o los daños surgidos de la información contenida en este documento.

Introducción

Sobre el presente documento

Este documento describe el fundamento para un enviar un respaldo de su información electrónica fuera de su centro de procesamiento, a lo que se conoce como un sitio externo u "offsite", como parte de una estrategia integral de prevención de contingencias o continuidad empresarial.

El presente documento también delinearé las opciones disponibles cuando se implementa una estrategia de respaldos "offsite", con el objetivo de lograr la mejor protección posible.

Quien debe leer este documento?

El presente documento debe ser leído por todas las personas responsables por el diseño y la implementación de una estrategia de protección de datos con respaldo en un sitio externo.

También debe de ser útil para aquellos planeando e implementando sistemas de respaldo.

Indice

Introducción	6
La Necesidad de Respaldo	6
Tipos de Respaldo.....	7
Respaldo a Nivel de Aplicación	7
Respaldo a Nivel del Sistema	8
Implementando una Estrategia de Respaldo	9
Asignando Personal Calificado	9
Definiendo los Requerimientos de la Empresa	10
Diseñando una Metodología de Respaldo	10
Seleccionando Tecnología de Respaldo	11
Implementando Tecnología de Respaldo	11
Implementando un Programa de Respaldo Fuera de Sitio	12
Implementando un Programa de Pruebas de Recuperación	12
Incorporando la Estrategia de Respaldo al Plan de Recuperación de Desastres	12
Implementando una Estrategia Fuera de Sitio	13
Como pueden ser las Unidades de Media enviadas Fuera de Sitio ?.....	14
Asegúrese de que los Catálogos del Sistema de Respaldo se encuentran claramente identificados y almacenados Fuera de Sitio	15
Asegúrese de que todos los Volúmenes posibles sean enviadas Fuera de Sitio	15
Asegúrese de que los Volúmenes de Unidades de Media correctos sean los que son enviados Fuera de Sitio	16
Pre-Identifique los Volúmenes requeridos para su recuperación	16
Asegúrese de que el Equipo de Respaldo recibe el mantenimiento adecuado	16
Envíe los Respaldos Fuera de Sitio tan pronto como sea posible	17
Envíe los Respaldos Fuera de Sitio tan frecuentemente como sea posible	17
Siempre coloque el Código de Barras en la Unidad de Media, no en la Caja de la Unidad ..	17
No encierre las Unidades de Media en contenedores	17
Minimize la Recuperación de Volúmenes Fuera de Sitio	18
Nunca recupere todos los Puntos de Restauración	18
Minimize la exposición a los cambios ambientales	18

Minimize la exposición a temperatura y humedad extremas	19
Minimize la exposición a contaminantes.....	19
Las Unidades de Media deben de ser transportadas en contenedores firmemente sellados para evitar la contaminación por polvo	19
Proteja las Unidades de Media de fuerzas tales como las caídas	19
Mantenga la Cadena de Custodia	20
Transporte las Unidades de Media en Vehículos que no atraigan la atención excesiva	20
Almacene las Unidades de Media Fuera de Sitio en un ambiente limpio, ambientalmente controlado	20
Proteja las Unidades de Media de los altos niveles de EMR y de los campos magnéticos.....	21
Almacene las Unidades de Media en un Espacio de Riesgo Calculado	21
Almacene las Unidades de Media en un espacio con protección contra el fuego y sistemas de detección y supresión del mismo	21
Lleve a cabo revisiones de antecedentes criminales sobre todos los integrantes del personal que manejen las Unidades de Media	22
Mantenga la localización Fuera de Sitio y la información Fuera de Sitio de los Asociados bajo una base de necesidad de conocimiento.....	Error! Bookmark not defined.
Implemente una jerarquía de autorización para las solicitudes de recuperación de Unidades de Media Fuera de Sitio	23
Eligiendo un Asociado Fuera de Sitio	24
Indice	25

Introducción

En 1936 fue desarrollada en Alemania lo que ahora nosotros conocemos como la moderna computadora por Konrad Kuse. Tras 70 años de constante desarrollo de la tecnología computacional, hemos alcanzado como resultado una economía global que es ahora dependiente del acceso a la información altamente actualizada.

Con el desarrollo de la computadora personal en 1981, y la adopción dominante del Internet debido principalmente a la Red Internacional, el acceso ininterrumpido a un mundo de datos públicos y de propiedad es ahora considerado por muchos como un derecho.

A pesar de que las computadoras modernas son sustancialmente más confiables que sus tempranos antecesores, su operación continua no está garantizada. Esto se debe principalmente al hecho de que el ciclo de desarrollo de la vida de una computadora se encuentra principalmente marcado por las expectativas del consumidor de incrementar constantemente su funcionalidad y enfocarse menos a una confiabilidad mejorada.

Puesto que siempre existirá una necesidad constante por computadoras que provean nueva y mejorada funcionalidad, el riesgo de fallas en el sistema siempre estará presente.

Nunca debe existir la expectativa de que las computadoras van a ser completamente confiables. Después de todo, aún los sistemas computacionales más avanzados concebidos por la ciencia ficción de Hollywood inevitablemente se volvieron locos. Fueran los sistemas de HAL de 2010, la Red Sky de la Trilogía de Terminator o Yul Brynner como el pistolero en WestWorld, todas estas fueron caracterizaciones de la falibilidad de la tecnología.

La Necesidad de Respaldo

El respaldo siempre ha sido la estrategia primaria para la protección de los datos de computadora.

Con la creciente popularidad de la computación distribuida, se han desarrollado nuevos riesgos tales como la piratería informática (hacking), los virus y la utilización

indebida (mal-ware). Cada uno de estos ha sido atacado parcialmente con contramedidas tales como la encriptación, los muros (firewalls) y el software de protección contra virus.

Estos riesgos evolucionan constantemente para minar cualquier avance logrado en la protección.

Por esta razón es que el Respaldo sigue siendo la única forma viable para la protección de datos.

Tipos de Respaldo

Los respaldos pueden ser esencialmente divididos en dos categorías, estos son: respaldos a nivel de aplicación y respaldos a nivel de sistema. A pesar de que existe frecuentemente una sobre-posición en estos tipos de respaldo, cada uno de ellos cumple una función discreta y determinada.

Respaldo a Nivel de Aplicación

El respaldo a nivel de aplicación es realizado para proteger la información a un nivel de archivo o registro y debe de ser realizado a intervalos regulares dentro del proceso y operación diaria.

En caso de existir un peligro por corrupción o borrado, la función primaria del respaldo a nivel de aplicación es el proveer un punto para la restauración de los archivos individuales.

En algunos casos estos respaldos también son utilizados para actualizar registros después de una restauración total del sistema, ya que frecuentemente son más recientes que el conjunto del respaldo total. La opción de utilizar estos puntos de restauración en caso de desastre puede ser que solamente sea accesible si una copia de estos respaldos ha sido enviada fuera de sitio.

Respaldo a Nivel de Sistema

El respaldo a nivel de Sistema es realizado para proteger la información a nivel de un equipo o una empresa y frecuentemente se realiza antes o después de periodos cercanos a los días de procesamiento o antes de cambios mayores en el sistema.

La función primaria de los respaldos a nivel de sistema es el proveer un punto de restauración a partir de cero o "Bare Metal" en el caso de que se dañe o pierda significativamente un sistema o empresa completa.

Es esencial que estos respaldos sean sacados de línea y enviados fuera de sitio, esto es a una ubicación distinta, para asegurar que ellos no estén en riesgo y se encuentren accesibles en caso de que sean requeridos.

Implementando una Estrategia de Respaldo

El implementar una estrategia de respaldo es una tarea muy compleja. Requiere una comprensión clara y completa de los sistemas computacionales y de las reglas de negocios que pocas veces son comunes entre una empresa y otra.

A pesar de la complejidad de la tarea, la planificación de la estrategia de respaldo habitualmente adolece de una fundamentación pobre, ya que es común que el peso del diseño de la misma sea delegado a un equipo que no está en la posición necesaria para comprender los requerimientos de la empresa y las consecuencias asociadas con una estrategia errónea.

Los pasos básicos involucrados en el diseño e implementación de una estrategia de respaldo son:

- ü Asignación de personal calificado con una comprensión amplia de los sistemas de información de la empresa, de las metodologías de respaldo y de las mejores prácticas de respaldo.
- ü Definición de los requerimientos de la empresa y las expectativas de recuperación.
- ü Diseño de una metodología de respaldo que incluya un plan de prueba.
- ü Selección de la tecnología de respaldo que cumpla con los requerimientos de la empresa.
- ü Implementación de la tecnología de respaldo.
- ü Implementación de un programa de custodia de respaldos fuera de sitio.
- ü Implementación de un programa de prueba de recuperación.
- ü Incorporación de la Estrategia de Respaldo al Plan de Recuperación de Desastres (DRP) o Plan de Contingencias.

Asignando Personal Calificado

La asignación de personal adecuado es frecuentemente un reto en las empresas que tienen un sistema complejo. Con frecuencia, precisamente las personas que serían necesarias para implementar un plan, se encuentran ya ocupadas en otros proyectos debido a la alta demanda existente por sus habilidades técnicas y su comprensión sobre la empresa.

Es crítico que los recursos apropiados sean asignados en todas las etapas del diseño del sistema de respaldo y en su implementación. En el caso de que el personal calificado no se encuentre disponible, puede ser necesario el traer personal externo que se especialice en el trabajo de respaldo para trabajar con el personal disponible, en el diseño de una estrategia.

Definiendo los requerimientos de la empresa

Una vez que los recursos adecuados han sido asignados a un proyecto, es básico que la empresa identifique sus requerimientos de negocio en relación con la recuperación.

Esto tradicionalmente ha sido asociado con aplicaciones específicas, pero cada vez más se asocia con requerimientos reglamentarios introducidos por los impuestos, la contraloría corporativa y la legislación privada.

También es importante el establecer las expectativas de negocio de la recuperación.

Como en todos los aspectos de los sistemas de información, casi cualquier cosa es posible cuando se está dispuesto a pagar el precio necesario. Dejando de lado las obligaciones derivadas de la legislación, depende de las unidades de la empresa el definir lo que están dispuestos a pagar para que pueda ser valorado frente a un riesgo aceptable asumido de pérdida de algunos datos. Una vez que las expectativas han sido claramente definidas, estas pueden ser eventualmente incorporadas a los Acuerdos de Nivel de Servicios (SLAs) y al Plan de Recuperación de Desastres (DRP) existentes.

Diseñando una metodología de Respaldo

El diseño de una metodología de respaldo es una labor altamente técnica ya que requiere del conocimiento de las tecnologías existentes y emergentes, así como una comprensión de las herramientas y metodologías que pueden ser aprovechadas.

Una vez establecida, una estrategia de respaldo tomará varios meses, (si no años) para perfeccionarse. Es por tanto de gran importancia el sopesar las metodologías probadas frente a la necesidad de una estrategia a prueba del futuro. En la

implementación de ambos respaldos a nivel de aplicación y de sistemas, se puede utilizar una combinación de las siguientes tecnologías:

- Ø Tecnología de Respaldo en espejo (Shadow Copy Technologies).
- Ø Respaldos incrementales basados en discos utilizando productos tales como DFHSM o cinta virtual.
- Ø Respaldos basados en cintas.

Seleccinando la Tecnología de Respaldo

Existen literalmente cientos (si no es que miles) de tecnologías de respaldo en el mercado hoy en día.

Estas tecnologías varían en precio desde gratuitas hasta de cientos de miles de dólares.

Una descripción de las opciones disponibles va más allá de los alcances de este documento, pero algunas de las tecnologías a considerar son:

- Ø Tecnologías de Disco (SAN's, NAS, iSCSI).
- Ø Sistemas de Archivos Distribuidos (Samba, SMB, NFS).
- Ø Tecnologías de Controlador de Cintas (DLT, LTO, AIT).
- Ø Tecnologías de Controlador Óptico (CDROM, DVD).
- Ø Automatización del Controlador de Cintas.
- Ø Software de Respaldo.
- Ø Software para mantener el registro de Cintas

Implementando Tecnología de Respaldo

Si no tiene implementada una estrategia de respaldo, el hacerlo debe ser una prioridad para su empresa.

Frecuentemente, las soluciones de respaldo requieren un trabajo de integración de sistemas significativo, así como la capacitación al personal para su operación. A pesar de que frecuentemente se pasa por alto y esto debe de ser sopesado frente a la necesidad urgente de implementar una solución de respaldo, es de gran importancia que se cambien las prácticas de administración y control de cambios que se llevan a cabo, después de que se implementa una solución de respaldo.

Implementando un Programa de Custodia de Respaldos Fuera de Sitio

Una vez que se ha implementado una solución de respaldo, es básico que los medios en que se realiza el respaldo a nivel de sistema y opcionalmente algunos respaldos a nivel de aplicación, sean sacados de las instalaciones de la empresa y enviados a un sitio externo.

Implementando un Programa de Pruebas de Recuperación

Independientemente de la fuerza de cualquier solución de respaldo, es crítico que la habilidad para restaurar sea probada con regularidad. La viabilidad de los respaldos a nivel de aplicación es frecuentemente probada de manera regular en la operación diaria, pero la viabilidad nunca debe de ser asumida.

Se recomienda que los respaldos del nivel de aplicación sean probados al azar por lo menos dos veces por año.

Se recomienda así mismo que se pruebe una vez por año una restauración total del sistema para todos los sistemas.

Cuando realice pruebas de recuperación asegúrese de probar su estrategia de custodia de respaldos en un sitio externo así como la respuesta de su proveedor externo.

Incorporando la Estrategia de Respaldo al Plan de Recuperación de Desastres.

Una Estrategia de Respaldo de Sistemas de Información es solo una parte de un Plan de Recuperación de Desastres (DRP) de la empresa.

Asegúrese de que la Estrategia de Respaldo se encuentra incorporada en el DRP de tal forma que se mantenga durante las revisiones del DRP.

Implementando una Estrategia Fuera de Sitio

Es básico que, como mínimo, los respaldos a nivel de sistemas sean enviados fuera de sitio a una ubicación que se encuentre lo suficientemente lejos de los datos primarios para mitigar los riesgos identificados.

Si los datos de respaldo han sido escritos en unidades extraíbles, las unidades pueden ser físicamente transportadas fuera de sitio. En algunos casos también puede ser posible el enviar estos datos fuera de sitio vía Internet público o a través de una línea de acceso privado.

Existen ventajas y desventajas en ambos métodos. No es la forma en que los datos llegan a estar fuera de sitio lo que representa el tema crítico; es la forma en que estos datos son almacenados y la forma en que pueden ser recuperados.

Por encima de esto, es crítico el que los datos se encuentren almacenados tanto fuera de línea, como fuera de sitio. Esta es la única forma de proteger la integridad de los datos.

También es una importante consideración el que los datos puedan ser localizados, regresados y restaurados de una forma muy expedita.

Como deben ser las Unidades de Media enviadas Fuera de Sitio?

Se debe de comprender que al enviar las unidades removibles fuera de sitio, usted está introduciendo de manera ineludible un nuevo riesgo a su empresa. Este riesgo, sin embargo, debe de ser evaluado frente a los requerimientos de proteger a la empresa de una pérdida total de datos. Por lo tanto, es esencial que cuando usted envíe estas unidades fuera de sitio, usted :

- ü Se asegure que los catálogos del sistema de respaldo se encuentran identificados claramente y almacenados fuera de sitio.
- ü Se asegure que todos los volúmenes de unidades seleccionados han sido enviados fuera de sitio.
- ü Se asegure de que los volúmenes de unidades correctos son enviados fuera de sitio.
- ü Pre-identifique los volúmenes necesarios para su recuperación.
- ü Se asegure de que el equipo de respaldo recibe el mantenimiento adecuado.
- ü Envíe los respaldos fuera de sitio tan pronto como sea posible.
- ü Envíe los respaldos fuera de sitio tan frecuentemente como sea posible.
- ü Siempre aplique el marcaje de barras en las unidades de media y no en las cajas.
- ü No ponga bajo llave las unidades en contenedores.
- ü Cuando sea posible, minimice la recuperación de los volúmenes de unidades que deben encontrarse fuera de sitio.
- ü Nunca recupere a la vez todos los puntos de restauración.
- ü Minimice la exposición de las unidades de media a los cambios ambientales.
- ü Minimice la exposición de las unidades de media a temperaturas y a humedad extremas.
- ü Minimice la exposición de las unidades a contaminantes tales como el polvo.
- ü Proteja a las unidades de las fuerzas excesivas tales como las caídas.
- ü Mantenga una cadena de custodia para cada una de las unidades de media.
- ü Transporte las unidades de media en vehículos que no atraigan la atención hacia el material que está siendo transportado.
- ü Almacene las unidades fuera de sitio en un ambiente limpio con control ambiental.
- ü Proteja las unidades de altos niveles de radiación electro-magnética (EMR) y de los campos magnéticos.
- ü Almacene las unidades en un espacio de riesgo calculado.

- ü Almacene las unidades en un espacio con protección contra el fuego y sistemas de detección y supresión del mismo.
- ü Lleve a cabo revisiones de antecedentes penales sobre todos los integrantes del personal que maneje las unidades.
- ü Informe la localización y proveedor de las unidades almacenadas fuera de sitio, únicamente a las personas que requieren conocerlo.
- ü Implemente una jerarquía de autorización para las solicitudes de recuperación de unidades de media fuera de sitio.

Asegúrese de que los catálogos del sistema de respaldo se encuentren claramente identificados y almacenados fuera de sitio.

En el caso de una "Restauración Bare Metal" o a partir de cero, será necesario primero el restaurar los catálogos de respaldo para facilitar la subsiguiente restauración de los sistemas de aplicación y de datos.

Asegúrese de que los catálogos de respaldo se encuentran claramente identificados y almacenados fuera de sitio. En caso de que su sistema apoye la creación de un pequeño catálogo de "archivos de arranque", estos archivos también deberán ser enviados fuera de sitio electrónicamente.

Asegúrese de que todos los Volúmenes seleccionados son enviados Fuera de Sitio.

Es básico que todos los volúmenes requeridos para la restauración de cada sistema sean correctamente identificados y enviados fuera de sitio.

Muchos Sistemas de Administración por Cintas (TMS) tienen la capacidad de identificar que volúmenes deben de ser enviados fuera de sitio o en su lugar cuales volúmenes se requerirían para restaurar un sistema en específico. Una vez que los volúmenes han sido identificados, ellos deberán ser comparados con las unidades de media que de hecho se están enviando fuera de sitio por medio de la utilización de escáners de código de barras y también compararlos frente a un inventario conocido cuando estos lleguen a su ubicación fuera de sitio.

Asegúrese de enviar fuera de sitio los Volúmenes de Unidades de Media correctos.

Una vez que han sido identificados, es básico que los volúmenes de unidades correctos sean enviados fuera de sitio. No es suficiente el presumir que algunos volúmenes han sido enviados fuera de sitio, o ni siquiera que una cantidad correspondiente de volúmenes ha sido enviada fuera de sitio.

Todos y cada uno de los volúmenes de unidades deben de ser cotejados frente al inventario conocido de cintas que debían ir fuera de sitio (conocido como lista de distribución).

Pre-Identifique los volúmenes requeridos para su recuperación.

No se espere a recibir un requerimiento de recuperación para identificar cuales respaldos son necesarios para la restauración. En una situación de desastre, el personal requerido para tomar estas decisiones podría no estar disponible, y en las empresas grandes este proceso puede, por si mismo, tomar varios días en completarse.

Muchos sistemas de administración de cintas proveen de reportes que pueden predecir que volúmenes serán necesarios para la restauración de cada sistema. Estos reportes deben ser programados para correr cuando los respaldos estén terminados. Los reportes deberán entonces ser transmitidos fuera de sitio.

Asegúrese de que el equipo de respaldo recibe el mantenimiento adecuado.

El equipo de respaldo, tales como los lectores de cinta magnética, deben de recibir el mantenimiento adecuado. Asegúrese de que los contratos de servicio están al día y de que las unidades son limpiadas en los intervalos especificados por el fabricante.

Envíe los Respaldos Fuera de Sitio tan pronto como sea posible

Mientras más pronto los volúmenes sean removidos fuera de sitio, menor es el riesgo potencial para la pérdida de datos. Los volúmenes de unidad de media deben ser llevados fuera de sitio tan pronto como sea posible después de que han sido recopilados.

Envíe los Respaldos Fuera de Sitio tan frecuentemente como sea posible.

Aún en las empresas pequeñas el costo de la pérdida de datos es extremadamente alto. En el caso de una completa falla en el sistema o de corrupción, los únicos puntos de restauración disponibles pueden ser aquellos que se encuentran fuera de sitio.

En sistemas de información altamente activos puede ser necesario el enviar las unidades de media fuera de sitio múltiples veces al día, sin embargo en la mayoría de los casos se recomienda que las unidades sean enviadas fuera de sitio una vez al día o por lo menos una vez a la semana.

Siempre coloque el Código de Barras en la Unidad de Media, no en la caja de la unidad.

Asegúrese de colocar los códigos de barras u otras etiquetas de identificación en los volúmenes de las unidades y no en las cajas de las unidades. Esto asegurará que ningún volumen equivocado sea enviado involuntariamente fuera de sitio en el caso de que la unidad de media sea colocada en la caja errónea.

No encierre las Unidades en Contenedores

Uno de los más altos riesgos de falla en la restauración se debe a un error interno del empleado. El encerrar las unidades de media en contenedores bajo llave coloca la

carga completa de administración de unidades sobre personal que puede estar ocupado con otras operaciones diarias.

El encerrar las unidades en estuches hace que la administración de los volúmenes de unidades de media no sea clara ante su proveedor externo.

Cuando usted envía sus unidades de media fuera de sitio, usted debe de permitir que tales unidades sean manejadas por su proveedor externo.

Minimice la recuperación de volúmenes fuera de sitio

Los respaldos fuera de sitio deben de permanecer fuera de sitio tanto como sea posible mientras contengan puntos de restauración viables. En donde sea posible, evite el recuperar los respaldos que se encuentran fuera de sitio. En el caso de que se requiera utilizar uno de los volúmenes que se encuentran fuera de sitio, únicamente solicite los volúmenes que sea necesario recuperar. No solicite volúmenes que no sean necesarios para la operación de restauración.

Si los volúmenes están siendo recuperados bajo una base regular, usted debería revisar su estrategia de aplicación de respaldos para determinar si no es necesario el mantener un esquema más amplio de respaldo dentro del sitio.

Nunca recupere todos los puntos de restauración

Siempre asegúrese de que por lo menos uno de los puntos de restauración permanece fuera de sitio. En el caso de que el único punto de restauración disponible permanezca fuera de sitio, puede ser necesario el duplicar los volúmenes, si el tiempo lo permite, antes de recuperarlo de su localización fuera de sitio.

Minimice la exposición a cambios ambientales

Deben evitarse los cambios ambientales tales como las variaciones en la temperatura y en la humedad. Las unidades deben de ser transportadas en un contenedor que

sea cerrado antes de que la cinta sea movida. La unidad debe ser mantenida y transportada en un vehículo de temperatura controlada.

Minimice la exposición a temperaturas y humedad extremas.

Las altas temperaturas pueden degradar la señal codificada de las unidades de media y dar por resultado fallas en la restauración de datos. Adicionalmente, los altos niveles de humedad pueden dar como resultado la creación de humedad y condensación.

Minimice la exposición a contaminantes

Los contaminantes tales como el polvo pueden causar daños en las unidades de media, pero también pueden dañar los equipos de lectura de las unidades tales como los lectores de discos o "drives". Existe también un riesgo de una contaminación cruzada cuando se utiliza una unidad contaminada en un lector en el que se ha utilizado previamente un volumen ya contaminado.

Las Unidades deben de ser transportadas en contenedores firmemente sellados para evitar la contaminación por polvo.

Cuando sea posible, asegúrese de que las cajas protectoras originales de las unidades de media sean utilizadas cuando se transportan y se almacenan las unidades fuera de sitio. Estas cajas han sido específicamente diseñadas para proteger la tecnología de las unidades con las cuales han sido entregadas.

Proteja las unidades de Media de Fuerzas tales como las Caídas.

La caída de las cintas puede dar como resultado la ruptura de la caja de la cinta, pero más críticamente puede también dar como resultado la ruptura de la orilla de la cinta. Las cintas de alta definición pueden dañarse seriamente por golpes o ruptura de la orilla de la cinta.

Las unidades de media deben de ser transportadas con gran cuidado para asegurar que estas no se caigan. Las unidades de media deben de ser mantenidas en el interior de contenedores que eviten que los volúmenes se golpeen entre ellos.

Los contenedores de transportación deben ser acomodados de tal forma que se eviten los impactos contra otros contenedores en el vehículo.

Mantenga la cadena de custodia

Asegúrese de que en cada etapa del ciclo de vida fuera de sitio se realice un completo seguimiento de auditoría que muestre quien, donde y cuando manejaron las unidades de media.

Cada vez que la custodia de las unidades de media cambie, asegúrese de que los mecanismos correspondientes se encuentren en funcionamiento para registrar el cambio.

Transporte las unidades de media en vehículos que no atraigan la atención excesiva.

Las unidades de media deben de ser transportadas en vehículos que no llamen la atención excesiva hacia el hecho de que están transportando datos críticos e importantes.

Almacene las unidades de media fuera de sitio en un ambiente limpio, ambientalmente controlado.

Asegúrese de que el edificio en el que sus unidades de media están siendo almacenadas está limpio y cuenta con los controles ambientales apropiados.

Se requiere el aire acondicionado para mantener una temperatura constante.

En los climas fríos puede ser necesario el humidificar el ambiente y en climas templados puede ser necesario el controlar la humedad del medio ambiente.

Proteja las unidades de media de los altos niveles de radiación electro-magnética (EMR) y de los campos magnéticos.

Los altos niveles de radiación electro-magnética y los campos magnéticos pueden llevar a la pérdida de señal en las cintas.

Se debe de tener especial cuidado en asegurar que las unidades de media sean transportadas y almacenadas bajo condiciones que no expongan a las cintas a EMR ni a campos magnéticos.

Almacene las unidades de media en un espacio de riesgo calculado.

El espacio en el que deben de ser almacenadas las unidades de respaldo debe de ser un espacio de riesgo calculado. Los puntos de riesgo pueden ser:

- ü Proximidad al sitio en donde los datos originales están almacenados.
- ü Proximidad a actividades de riesgo tales como estaciones de gas o reactores.
- ü Taza de crímenes en la localidad.
- ü Altura sobre el nivel del mar y riesgo de una inundación.
- ü Proximidad a la carga de combustibles.
- ü Proximidad hacia rutas alternativas de transporte.

Almacene las unidades en un espacio con protección contra el fuego y sistemas de detección y supresión del mismo.

En el caso de que ocurriese un fuego dentro o en los alrededores de la bóveda, es básico que la ubicación de almacenaje cuente con los mecanismos apropiados de control de fuego.

Estos mecanismos no deben colocar a las unidades de media en una situación de riesgo que ellos mismos causen. Por esta razón se deben de evitar los rociadores de agua.

Lleve a cabo revisiones de antecedentes penales sobre todos los integrantes del personal que maneje las unidades de media

Es indispensable que todo el personal que maneje las unidades de media pase por una revisión de sus antecedentes penales para asegurarse de que no tienen tendencias criminales que pudiesen hacer inapropiado el que ellos se encuentren expuestos a información y datos de alto valor.

Informe la localización y proveedor de las unidades almacenadas fuera de sitio, únicamente a las personas que requieren conocerlo.

El almacenaje de la información y datos fuera de sitio debe de ser visto como una medida preventiva al sabotaje. Por esta razón es básico que la información sobre la localización de los datos fuera de sitio y del proveedor externa sea proporcionada únicamente a aquellas personas que requieren saber esta información para la ejecución de sus funciones.

Asegúrese de que todas las partes que saben la localización y los detalles sobre el proveedor han aceptado el no revelar estos detalles a otras personas a través de la firma del Acuerdo de Confidencialidad.

Asegúrese de que ningún proceso público de oferta revele de forma inadvertida esta información.

Implemente una jerarquía de autorización para las solicitudes de recuperación de unidades de media fuera de sitio.

Es indispensable que únicamente cierta parte del personal dentro de la organización tenga la autoridad para recuperar los puntos de restauración que se mantienen en los espacios fuera de sitio. Por lo tanto es necesario que usted determine una jerarquía de control de acceso que defina el personal que puede recuperar las unidades de media, así como quien puede promover y remover otros accesos para la recuperación de dichas unidades de media.

Eligiendo un Proveedor Externo

Para muchas empresas, el concepto de entregar todos sus datos críticos a un proveedor representa un riesgo por si mismo. A pesar de que existe algo de cierto en esta idea, no se diferencia demasiado de nuestros abuelos guardando su dinero bajo el colchón en lugar de confiar en la credibilidad de un banco. Existen beneficios considerables en tener sus unidades de media críticas almacenadas por un Proveedor Externo, cuando se le compara con la alternativa de tener a un empleado que se lleve a casa estas unidades, con almacenarlas en una caja fuerte en el lugar o con entregarlas a un banco. Algunas de estas ventajas son:

- ü El que las unidades de media sean administradas por alguien que es un experto en el campo.
- ü Contar con la confianza de una recolección puntual.
- ü Un acceso de 24 x 7 a las unidades de media.
- ü Las unidades de media son almacenadas fuera de sitio.
- ü Recuperación rápida de las unidades de media.
- ü Protección de sabotaje o robo por parte de los empleados.
- ü Consejos sobre temas tales como respaldo y continuidad empresarial.

Índice

Asesoramiento 17

Aire acondicionado, 15

AIT, 8

Respaldo a nivel de aplicación, 6

Respaldo a nivel de Aplicación, 6

camino de auditoría, 15

revisión de respaldo, 4, 11, 16

Respaldo, 3, 5, 6, 7, 8, 9, 12

Software de Respaldo, 8

codigos de barras, 12, 13

Bare Metal, 6

Bare Metal Restauración, 11

archivos, 12

requerimientos de negocios, 3, 7

CDROM, 8

cadena de custodia, 11, 15

condensación, 14

contenedores, 14

contenedores, 3, 4, 11, 13, 14, 15

gobierno corporativo, 7

corrupción, 6, 13

contramedidas, 5

contaminación cruzada, 14

borrado, 6

DFHSM, 8

Plan de Recuperación de Desastres, 9

respaldo basado en disco, 8

DLT, 8

DRP, 7, 8, 9

polvo, 4, 11, 14

DVD, 8

radiación electro-magnetica, 11, 15

EMR, 4, 11, 15

señal codificada, 14

encriptación, 5

fuego, 4, 11, 16

protección contra el fuego, 4, 11, 16

muros, 7

restauración del sistema, 6, 9

piratería, 5

cintas de alta tecnología, 14

humedad, 4, 11, 14

Internet, 5, 9

LTO, 8

mal-manejo, 5

NDA, 16

nuevos riesgos, 5

NFS, 8

Acuerdo de Confiabilidad, 16

Estrategia primaria, 5

legislación privada, 7

punto de restauración, 6, 13, 14

punto de restauración, 4, 6, 11, 13, 14,
16

avance, 6

Samba, 8

Acuerdo a nivel de servicio, 8

SMB, 8

respaldo a nivel de sistema, 7

respaldo a nivel de aplicación, 8

respaldo en cintas 8

Sistemas de Administración, 12

temperatura, 4, 11, 14, 15

TMS, 12

cinta virtual, 8

software de protección contra virus, 5

virus, 5

Red a Nivel Mundial, 5