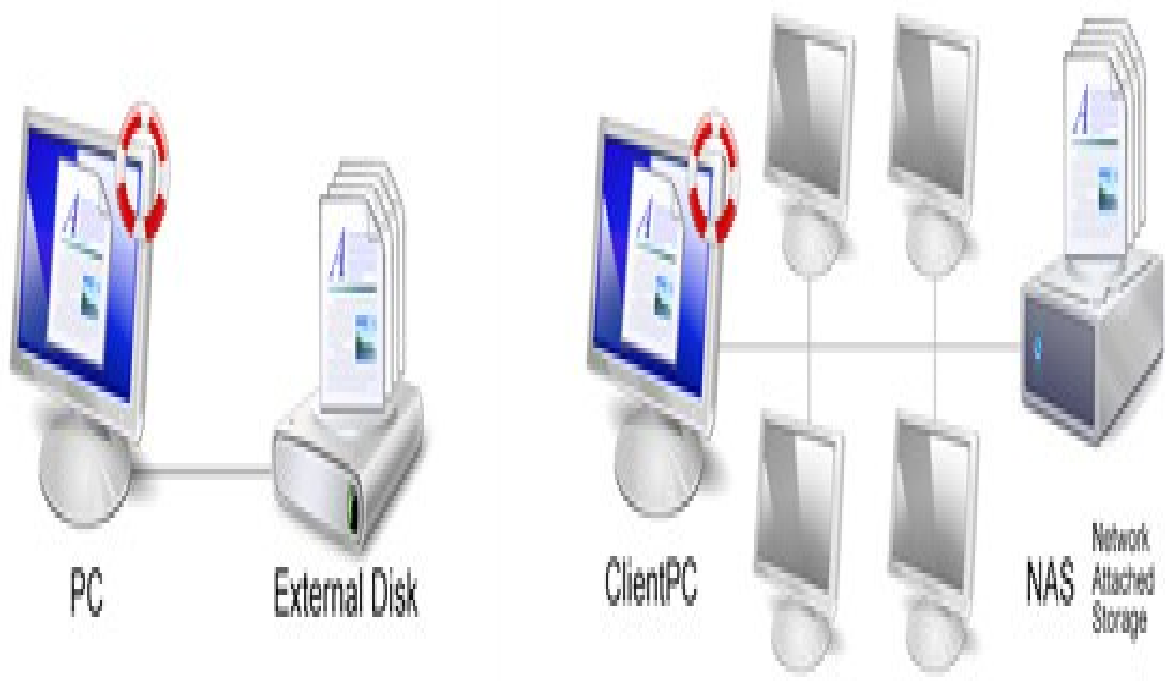
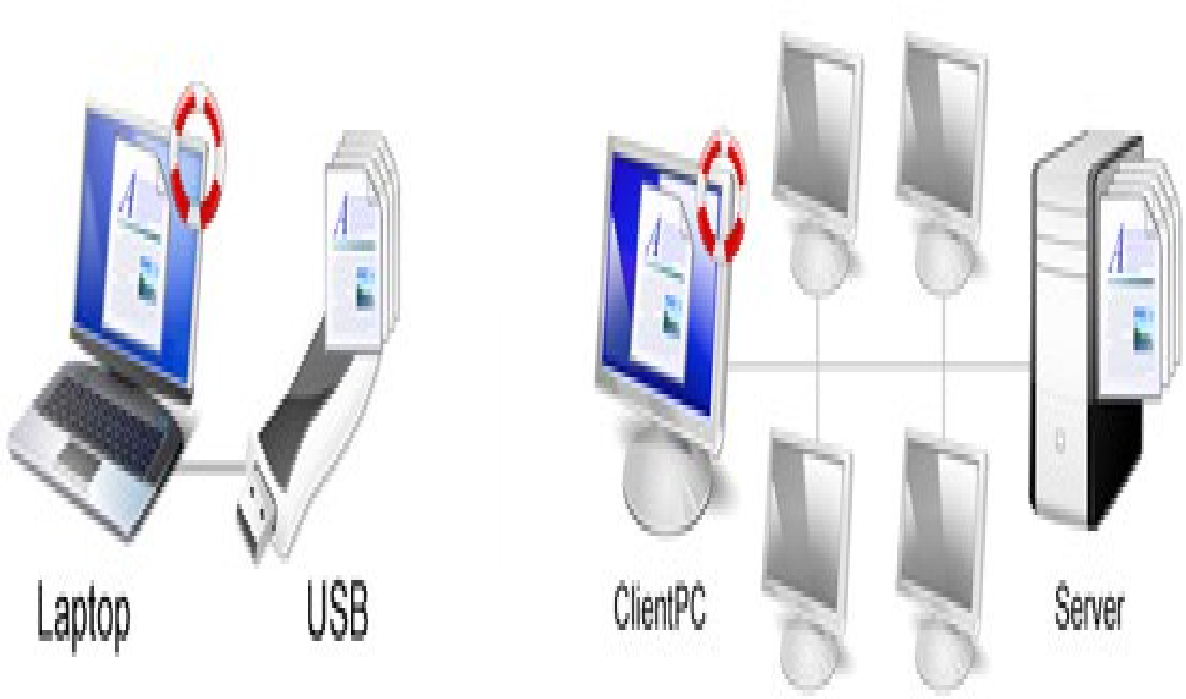
DOCUMENTO DE LA POLÍTICA
DE RESGUARDO DE LA INFORMACIÓN



Lineamientos y normativas para el respaldo de la información
de los usuarios de Opus Software®



Publicado por

Sector PMO & Gestión Documental de Opus Software®

Ultima revisión Abril, 2014

Información de Referencia	
Nombre del archivo y ubicación	OpusSoporteTecnico_DocumentodePoliticaRespaldo.doc ➔ En la WIKI en el capítulo Manuales de Usuario hay un link a este documento ➔ En Opuslx\documentacion\PMO
Fecha de Creación	28/11/2013
Autor	Opus Software® – PMO & Gestión Documental
Propósito	Descripción del servicio de resguardo de la información, con lineamientos y normativas propuestas para el desarrollo de dicha gestión
Ultima Revisión	22/04/2014

Indice de contenidos

PROPÓSITO 4
ALCANCE DE LA GESTION 4
OBJETIVO 4
RESPONSABILIDADES 4
LINEAMIENTOS Y DIRECTIVAS A CONSIDERAR 4
Seguridad física y ambiental 4
Gestión de entornos operacionales 5
Gestión de incidentes en el resguardo de la información 5
Planilla de Check List de incidentes 5
PROCEDIMIENTOS DE RESGUARDO Y RECUPERACION 5
Plan de resguardo 5
Cuales datos se deben incluir 5
Medios de soporte a utilizar 6
Herramienta de respaldo 6
Tipos de respaldo a implementar 6
Respaldos globales diferenciales 6
Respaldos parciales 6
Periodicidad de los respaldos 6
Esquema de conexión de resguardos 8
Diagrama de distribución de resguardos 8
Donde guardar las copias 7
Responsable del proceso de resguardo y recuperación 7
PLAN DE CONTINGENCIA DE RESPALDOS PARA RESTAURACIÓN DEL SISTEMA DAÑADO 8
Nuestro servicio para la contingencia 8
GLOSARIO DE TERMINOS 10

Propósito

Este documento tiene por propósito dar a conocer a los clientes la importancia y sensibilidad de resguardar la información que permite crecer y mantener competitiva a una empresa.
Esta información representa un activo de valor esencial para cualquier negocio u organización y la necesidad de minimizar los riesgos de pérdida o deterioro de la misma han llevado a que desarrollemos una gestión de resguardo de la información.
Dicha política representa un servicio que estamos en condiciones de ofrecer, consta de directrices para orientar en el uso adecuado de tecnologías de resguardo y un plan de buenas prácticas que ayudan a proteger adecuadamente los activos tecnológicos y la información de nuestros clientes.

Alcance de la gestión

Proporciona una herramienta de apoyo y asesoría para la planificación, organización, ejecución y control de las actividades para mejorar el resguardo y la recuperación de la información de las áreas informáticas de las organizaciones con la finalidad de salvaguardar el valioso activo que ella representa y asegurar la continuidad del procesamiento de datos.

Objetivo

Definir claramente las políticas de resguardo ofrecida con esta herramienta, delimitando las responsabilidades asumidas con este servicio. Se debe saber que ningún conjunto de controles puede lograr la seguridad completa, pero que sí es posible reducir al máximo los riesgos que amenacen con afectar la seguridad física o lógica de la información.
La política propuesta establece un conjunto de directrices y recomendaciones preventivas cuyo objetivo es minimizar en lo más posible los riesgos ante pérdida, robo o daño de la información que dependen de la falta de mantenimiento adecuado de resguardo y recuperación.
Estas políticas se encuentran alineadas con las normas estándar internacionales ISO/IEC 27002 sobre seguridad informática y la norma ISO/IEC 24762 sobre directivas para los servicios de recuperación de desastres en las tecnologías de la información.

Responsabilidades

El servicio brindado en esta herramienta, funcionalmente, es ordenar las actividades para respaldar lo mejor posible la información en copias confiables, completas y actualizadas, controlarla y ante algún problema recuperarla y opcionalmente brindar mecanismos de contingencia para la continuidad del procesamiento de los datos.
El servicio de protección y prevención contra amenazas de software malicioso ocasionados por virus o ataques que rompan la seguridad de un sistema por accesos no autorizados no está comprendido dentro de esta política de resguardo.
Pero no se debe pensar que únicamente personas pueden ser los causantes de estos daños, pues existen otros factores como los eventos naturales, que son capaces de desencadenar daños materiales o pérdidas inmateriales en los activos, y son también consideradas como amenazas. Los incendios, inundaciones, huracanes y el terrorismo son ejemplos más comunes que provocan esta situación. Incluimos en esta lista los desperfectos o fallos en alguno de los componentes de hardware relacionados con el servicio de respaldo.
Ante estos eventos haremos una serie de recomendaciones que ayudan a preservar la integridad de la información.

Lineamientos y directivas a considerar

Seguridad física y ambiental

Es recomendable contar con un área segura donde residan los equipos servidores y de resguardo que contienen la información y los medios de procesamiento. Respecto a las áreas seguras, se refiere a un perímetro de seguridad física que cuente con barreras o límites tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas, y medidas de esa naturaleza para proteger las áreas que contienen información y los medios de procesamiento de información.
Además de eso, es necesario considerar la seguridad física con respecto a amenazas externas y de origen ambiental, como incendios, para los cuales deben haber extintores adecuados y en los lugares convenientes, fugas de agua, o inundaciones.

En cuanto a la seguridad ambiental:
Se debe controlar la temperatura adecuada para los equipos.
Evitar ambientes contaminados de polvo o con humedad.
La seguridad y protección del cableado, los cables deben estar dentro de ductos y evitar ser aplastados por muebles u objetos.
Mantenimiento de equipos mediante limpieza y revisiones periódicas y estar conectados a unidades de corriente continua.
Se debe verificar y controlar el tiempo de vida útil de los equipos para que trabajen en condiciones óptimas y permitan implementar los mecanismos de resguardo planteados.

Gestión de entornos operacionales

Es completamente necesario tener un nivel de separación entre los ambientes de prueba de las aplicaciones y de operación de la gestión, así como crear un ambiente de contingencia para evitar problemas operacionales ya sea borrado de archivos por descuido de los usuarios, test que destruyan datos o programas u otro tipo de incidente.
Bajo el directorio /home/pruebas/unit0 se creará un entorno de pruebas con un contenido idéntico al /home/opus/unit0 pero con las versiones de testing para pruebas de aceptación de nuevas aplicaciones.

Gestión de incidentes en el resguardo de la información y verificación de respaldos

Los sistemas de resguardos de la información estarán bajo auditorías mediante monitoreo y se chequearan regularmente para verificar y validar el cumplimiento de los estándares de implementación de los resguardos.
Se establecerán por nuestra parte, mecanismos para monitorear y cuantificar el estado de los respaldos.
Estas acciones de seguimiento y control en la seguridad de los respaldos se implementará a partir de log de comparaciones de datos, verificación de la integridad de la información origen contra la información resguardada, comunicación automática de incidentes vía e-mail a nuestro departamento de soporte, planillas de chequeo del resultado de las fases del respaldo y de las acciones correctivas en caso de detectar y analizar las fallas en el respaldo, prueba de verificación de resguardos y recuperación de la información para validar su operatividad.
La prueba de verificación de resguardos consiste en ejecutar cualquier función de *Opus ERP* utilizando los programas y datos respaldados en el entorno físico de resguardo verificando su operatividad y comparando los resultados contra las mismas funciones de *Opus ERP* en el ambiente de producción.
Estas tareas se realizarán en visitas periódicas programadas según contrato del servicio. Además se incluye el monitoreo mediante la comunicación automática vía e-mail en caso de registrarse algún incidente en el proceso de respaldo. Se informará al cliente sobre el resultado de los controles del proceso de resguardo, por esta vía.

CONTROL DE PROCESOS DE RESGUARDO

FECHA: _____

Proceso	Realizado	No Realizado	Incidentes y Observaciones	
Backup de Opus ERP a NAS 1				
Backup de Opus ERP a NAS 2				
Backup de Opus ERP a Server Contingencia				
Backup parciales de usuarios a NAS 1				
Backup parciales de usuarios a NAS 2				
	Porcentaje	Cantidad de MB		
Espacio disponible en disco				
Procesos que finalizaron anormalmente:				
Nombre proceso	Tipo de actividad	Hora inicio	Hora fin	Incidentes y Observaciones	Firma

Procedimientos de resguardo y recuperación

Plan de respaldo

Es la etapa inicial, en la que se analiza el método más adecuado de resguardo según las características de criticidad de la información del cliente, sus aplicaciones, tipo de instalación y características de los usuarios. Además se hará inventario y clasificación de los activos, se definirán los medios donde realizar las copias, su rotación y ubicación y la topologia de la infraestructura a aplicar.

Cuáles datos se deben incluir

1. Backups del software de aplicaciones, compuesto por los programas de procesamiento de *Opus ERP*, y cualquier otro software de *Opus Software* que también trabaje con los datos, para producir los resultados con los cuales trabaja el usuario final.

2. Backups de los datos y de estructura de datos de los que forman parte bases de datos con los archivos e índices de la información esencial del negocio que es la que constantemente esta cambiando, tablas de validación, contraseñas, usuarios, roles y todo archivo necesario para el funcionamiento de los sistemas de información de la empresa y la pronta recuperación de los mismos en caso de fallas.
En cuanto a estos datos y estructuras nos referimos tanto a los pertenecientes a las aplicaciones de *Opus Software* como a cualquier otra aplicación residente en el servidor de aplicaciones.

3. Backups de archivos de usuarios que son los archivos utilizados por el personal de los distintos sectores de la empresa y que cambian de acuerdo a los patrones de uso de los usuarios.
La información y programas de los puntos 1 y 2 residen físicamente en la carpeta /home/opus/unit0 del servidor de datos, para ello coordinar con el instructor de la cuenta que datos pueden eliminarse para hacer más limpia la copia.
Esto puede incluir datos de subcarpetas ubicadas bajo /home/opus
Clasificar junto con los usuarios finales la información a respaldar residente en el servidor , así como la información de trabajo en modalidad mono usuario en cada uno de sus pc´s de acuerdo con su grado de sensibilidad y criticidad.
Para ello es responsabilidad de los usuarios propietarios de la información, almacenarla únicamente en el directorio de trabajo que se le asigne. Esto incluye información de bases de datos (en estos casos aplicar funciones a tales efectos), correo , planillas electrónicas, documentos, modelos de Pyramid y otras aplicaciones de interés de cada puesto de trabajo según su criticidad y valor.
Del mismo modo son los encargados de documentar y mantener actualizada la clasificación efectuada inicialmente junto con el personal de soporte técnico.

Medios de soporte a utilizar.

Opción 1

Se establecerá una base mínima de dispositivos confiables y robustos constituidos por diferentes medios de soportes de almacenamiento. Uno será un dispositivo de almacenamiento externo compuesto 1 discos duros de red (NAS Network Attached Storage) identificados por una dirección IP , el otro un dispositivo de almacenamiento externo con interfaz USB conectado al equipo servidor para contener una segunda copia (off-site) fuera del mismo edificio.

Opción 2

Una segunda opción es utilizar 2 dispositivos de almacenamiento externo del mismo tipo ya sea NAS o con interfaz USB conectados al servidor.
Otras opciones se discutirán con el cliente en caso de optar por pendrives o cintas no recomendables por nosotros por ser dispositivos de menor vida útil y menos confiables por su mayor probabilidad de error que los antes mencionados.

Herramienta de respaldo

Consiste en la implementación de un software de backup inteligente, configurado para actuar en forma automática ejecutando procesos de tareas programadas. Establece la fecha y horario de ejecución de los procesos de resguardo que copian la información a diversos soportes de respaldo y graban una auditoría de su ejecución y resultado de su completitud.

Tipos de respaldos a implementar

Respaldo global diferencial (full-backup) de la aplicación

Asegura la totalidad de los datos, inicialmente se realiza un backup total o global del /home/opus del servidor donde se encuentran los datos de la empresa y posteriormente se realiza una copia de los datos modificados después del último backup total realizado.
El régimen de copias se diario y semanal, esto significa que el respaldo se hace todos los días en un área física diferente (un área asignada a cada día de la semana de lunes a viernes) y además semanalmente se actualiza una copia contenida también en un áreas físicamente diferentes correspondientes a cada una de las semanas del mes.
Se asignan 2 dispositivos NAS en forma rotativa semanalmente. Cada viernes un dispositivo es sacado fuera de la oficina durante el período correspondiente a la semana siguiente y sustituido por el que anteriormente fue objeto de rotación.

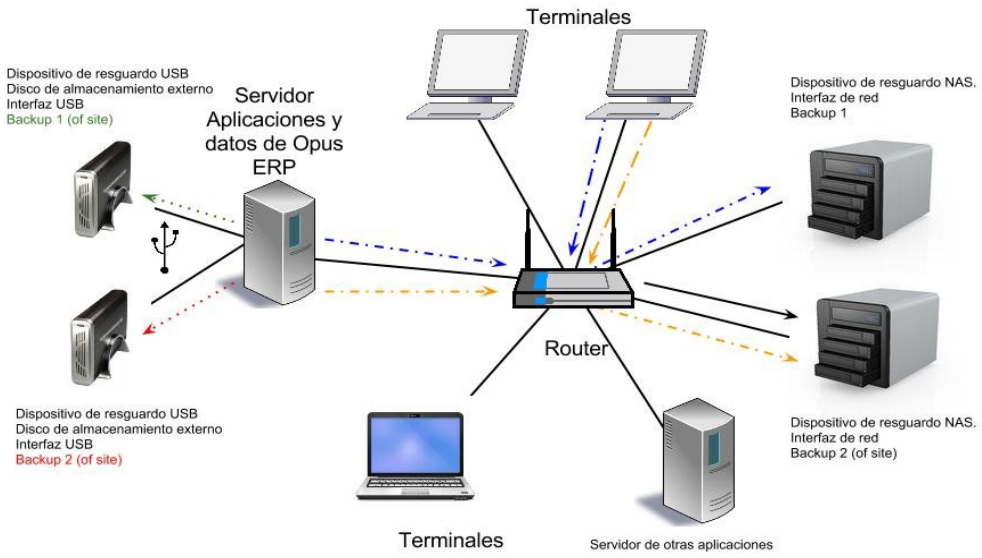
Respaldos parciales

Se llevan a cabo en los pc´s de cada usuario como se detallo en el punto “cuales datos se deben incluir”.
Se realizarán con el mismo esquema de respaldo que el respaldo global

Periodicidad

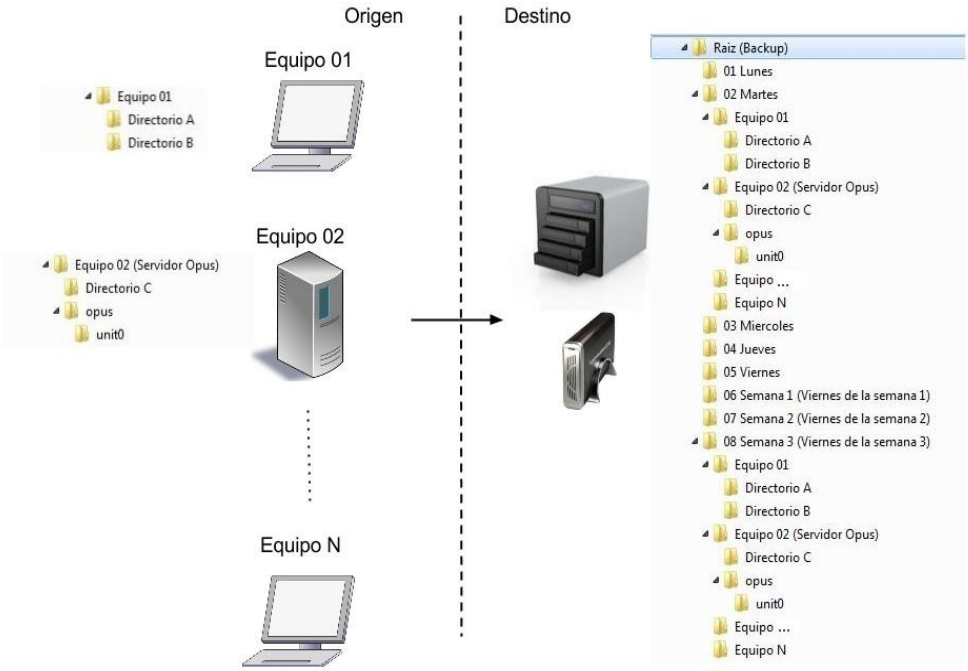
Lo usual y recomendable es realizar respaldos diariamente según el esquema dispuesto.
El momento de la ejecución del respaldo será en tareas nocturnas programadas que comienzan al final de la jornada de trabajo para no afectar los tiempos disponibles de procesamiento de datos de la empresa.

Esquema de conexión de resguardo



Nota:
Líneas amarillas y azules se aplican todos los equipos a resguardar

Diagrama de distribución de resguardo



Donde guardar las copias

Se recomienda guardar una copia bajo llave en un lugar en condiciones adecuadas y de fácil acceso inmediato y asignar a la o las personas que tienen acceso inmediato a dicha copia.
Otro juego de respaldo se guardará fuera del edificio, del mismo modo se asignará personal para acceder y restablecer en forma fluida dicha copia en caso de ser necesario.

Responsable del proceso de resguardo y recuperación

El responsable de la supervisión del funcionamiento del proceso de resguardo y su eventual recuperación será el Departamento de Soporte de Opus Software mediante los procedimientos de verificación del resultado del respaldo, control de auditorías y pruebas de recuperación en el régimen periódico establecido en el contrato de este servicio. Estas pruebas servirán para constatar que se puedan obtener correctamente los datos grabados en el soporte al momento de ser necesarios, de forma de garantizar su propósito.

Plan de contingencia y recuperación de respaldos para la restauración del sistema dañado

Contiene medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una empresa. Consiste en los pasos que se deben seguir luego de un desastre, para recuperar la capacidad funcional del sistema. Entendemos por recuperación *"tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema , como la posibilidad de volver a la situación anterior al mismo, habiendo recuperado el máximo posible de los recursos e información".*

Con nuestro servicio es posible

Proveer una opción para mantener operativas las plataformas informáticas de la empresa., que permita reducir el impacto en las operaciones normales de la empresa cuando son interrumpidas por la presencia de eventos que afectan las instalaciones donde se procesan sistemas.
Esto incluye *Opus ERP* y otras aplicaciones críticas o de sensible importancia para la empresa o usuarios finales.

Consiste en la puesta en marcha de una serie de acciones para restablecer la continuidad operativa del negocio.
Para ello previamente se identifican y evalúan el hardware, software, datos y aplicaciones críticos a ser protegidos y se define un entorno informático de contingencia. Este recurso puede lograrse con el inventario, clasificación y control de activos, se incluye entonces como estrategia, un inventario de sistemas, se identificarán los activos importantes de hardware y software asociados a cada sistema de información, sus respectivos propietarios y su ubicación. El inventario será una alternativa para la planeación de la recuperación de desastres.

Como resultado de la evaluación se definirá un entorno de contingencia que tendrá como base otro equipo con porte servidor, con una instalación espejo a la del servidor de Opus ERP y una estructura similar a la plataforma informática usual a la que se tendrá acceso de manera inmediata en caso de desastre.
Dicha instalación es actualizada diariamente para contener los datos necesarios para la contingencia por tal la vigencia de la data será del día anterior.
Para ello se implementarán técnicas de replicación automática, por hardware o software, de forma tal que si el equipo–base de datos principal deje de funcionar, el equipo–base de datos espejo tome el control inmediatamente después de coordinar las nuevas direcciones IP.
En caso de que algún evento cause una falla prolongada se podrá utilizar la instalación de contingencia.
En caso de falta de energía por tiempo prolongado , se suplirá la energía eléctrica mediante un sistema de emergencia previamente definido ya sea por UPS para proceder a las tareas de finalizar los procesos o por generador para continuar con algunas tareas críticas básicas.
En caso de falla en el funcionamiento del disco del servidor o cualquier otro elemento donde residen las aplicaciones y datos de producción:

a) conectar a todos o parte de los usuarios al equipo-base de datos espejo, para ello es necesario una operación simple de configuración para redireccionar la comunicación hacia la dirección IP del nuevo host, esto básicamente consiste en asignar al equipo-base espejo la dirección IP del servidor original.

b)tener disponibilidad inmediata e identificar fácilmente el disco NAS de respaldo.

c) restaurar la información afectada desde la copia de respaldo más reciente

d) se realiza una prueba de integridad de los datos para verificar si están las transacciones afectadas y se continua operando normalmente.

e) en caso de falla del backup 1 se recurrirá a la segunda copia off site y se repiten los pasos c) y d).

En estas situaciones deberá tomar recaudo la cadena de mando correspondiente dentro de la organización (coordinador de contingencias) comenzar con el plan de contingencia y comunicarse al Departamento de Soporte Técnico de *Opus Software* para que los responsables del proceso de resguardo comiencen a actuar.

El Servicio de Contingencia, tanto la infraestructura como el procedimiento y la Recuperación de Respaldos son opciones del servicio.

Glosario de términos

Activo Informático:
Un “Activo”, es todo elemento que compone todo el proceso de la comunicación, partiendo desde la información, emisor, medio de transmisión y receptor.

Amenaza:
Es cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Por ej:fallas en el suministro eléctrico, virus, sabotajes o usuarios descuidados.

Backup:
Es el proceso de copiar o salvaguardar la información en otra unidad, dispositivo, memoria, computador o servidor; con el objetivo de restaurarla fácilmente en el caso que se pierda por algún motivo.

Incidente:
Cuando se produce un ataque o materializa una amenaza, tenemos un incidente, como por ej. un intento de borrado de un archivo protegido.

Inventario, clasificación y control de activos:
Se fundamenta que las aplicaciones de negocios se encuentran distribuidas sobre muchos componentes de hardware en una área geográfica. Por tal es recomendable conocer que aplicaciones hay en cada puesto de trabajo y donde se ubica cada uno de ellos y las interrelaciones de los mismos para determinar la prioridad de su recuperación.
Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad, disponibilidad.
La información a resguardar se rotulará bajo una carpeta con un nombre especialmente identificatorio para tales efectos y ubicará en el equipo servidor y cada uno de los pc´s de los usuarios.
También se rotulará adecuadamente con una identificación (número nombre y ubicación), cada elemento inventariado y los dispositivos de soporte del respaldo (así se identificarán el equipo servidor y su ubicación y los dispositivos de soporte por ej), Este esquema de rotulado se documentará de manera que conste en una guiá o manual disponible en el momento de necesidad de recuperación.

Desastre:
Se considera como tal la interrupción durante un período considerable de tiempo de los recursos informáticos de una organización, durante el cual puede verse seriamente afectada en su operación y en su imagen de servicio. Los incendios, inundaciones, huracanes y el terrorismo son ejemplos más comunes que provocan esta situación.

Disponibilidad:
Se refiere a que la información esté disponible en el momento que se necesite

Estándar:
Los estándares son actividades, acciones, reglas o regulaciones obligatorias diseñadas para proveer a las políticas de la estructura y dirección que requieren para ser efectivas y significativas.

Norma o normativa:
Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización

Plan de contingencia:
Es un instrumento de gestión para el buen manejo de las tecnologías de la información y las comunicaciones en el dominio del soporte y desempeño..

Resguardo:
Archivos, equipo, datos y procedimientos disponibles para el uso en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.

Riesgo: Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene.

Seguridad de la Información:
La seguridad de la información se entiende como la preservación de las siguientes características:
• Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
• Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
• Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados
con la misma, toda vez que lo requieran.

Tecnología de la Información:
Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Universidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.