UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

FOLLETO DE ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

Dr. Vladimir Villarreal

2020

CONTENIDO

1. Introducción a la administración de los Sistemas operativos 5
1.1 Concepto 5
1.2 Etapas o secciones 5
1.3 Aspectos en la administración de un Sistema Operativo 5
1.4 Funciones del administrador 10
2. Administración de usuarios y grupos 15
2.1 Crear, añadir, modificar, eliminar usuarios 15
2.2 Controlar usuarios y sus contraseñas 18
2.3 Crear grupos de usuarios 21
2.4 Asignación de permisos 23
2.5 Compartiendo archivos 24
3. Administración de recursos del sistema, Monitorización y Mantenimiento 29
3.1 Rendimiento del Sistema y control de la CPU 29
3.2 Administración de la memoria 34
3.3 Servicios de la impresión 35
3.3.1 instalación y administración 37
3.4 Administración de terminales 40
3.5 Administración de módems 41
3.6 Otros dispositivos 42
4. Monitorización y mantenimiento 47
4.1 Gestión de almacenamiento en disco 47
4.1.1 Discos, volúmenes, particiones 48
4.1.2 Compresión de archivos 53
4.2 Gestión de las comunicaciones en la red 54
4.2.1 Protocolos 56
4.3 Técnicas y herramientas para gestión de redes 58
4.3.1 Consola remota, monitoreo, órdenes del servidor 58
4.4 Respaldo y recuperación de datos 60
5. Software de Aplicación 65
5.1 instalación de software de aplicación 68
6. Administración de archivos y respaldos 71

6.1 Archivos 73
6.2 Sistemas de gestión de archivos 74
6. 3 Organización y acceso archivos 77
6.4 Administración de archivos en ambientes de clúster y nubes. 81
7. Archivos y respaldos 88
7.1 Riesgo en los cuales se encuentran inmersos los Sistemas de Información 88
7.2 Clasificación de respaldos 89
7.3 Dispositivos de almacenamiento 92
7.4 Tecnologías: óptica y magnética u otras de almacenamiento 92
Bibliografía 101

CAPÍTULO I. INTRODUCCIÓN A LA ADMINISTRACIÓN DE SISTEMAS OPERATIVOS

Objetivos:

- Proporcionar un panorama general de la evolución conceptual de la administración de los sistemas operativos.
- Describir las etapas y secciones que involucra la administración de un SO.
- Listar las principales funciones de un administrador de SO.

¿De qué trata esta sesión de aprendizaje?

En esta sesión de aprendizaje se presentan conceptos fundamentales y las etapas que conlleva la tarea de administrar un sistema operativo; además se describen las funciones que debe llevar a cabo todo administrador de sistema operativo para lograr la eficiencia y eficacia del sistema.

1. Introducción a la administración de los Sistemas operativos

1.1 Concepto

La administración de un sistema incluye un amplia gama de tareas tales como las de instalar una impresora o un escáner, configurar y compartir el acceso a Internet, instalar programas, configurar un cortafuegos, añadir nuevos usuarios, etc., en definitiva crear un entorno de trabajo seguro, cómodo y productivo.

Igualmente, tiene por misión, garantizar el uso eficiente de los propios recursos y la seguridad, así como la disponibilidad, integridad y confiabilidad de la información.

Junto a todo esto, las operaciones de administración de sistemas también están encaminadas a proporcionar servicio de soporte técnico, solucionar problemas y la actualización de la documentación del propio sistema

La administración de sistemas operativos se apoya en muy diversos softwares que contribuirán al desempeño eficiente de la tarea en cuestión.

1.2 Etapas o secciones

Se puede dividir la administración de sistemas operativos en varias secciones:

- Administración de usuarios
- Administración de procesos
- Administración de discos
- Administración de red

1.3 Aspectos en la administración de un Sistema Operativo

Existen algunos aspectos a los que se les debe prestar especial atención a la hora de administrar los sistemas operativos; entre los que están:

- **La administración del almacenamiento día a día.** Los administradores del sistema deben prestar atención al almacenamiento en el curso de su rutina diaria. Hay varios problemas que se deben tener en cuenta:
  - ✓ Monitorizar el espacio libre
  - ✓ Problemas con cuotas de disco
  - ✓ Problemas relacionados a archivos
  - ✓ Problemas relacionados a directorios

- ✓ Problemas relacionados a respaldos
- ✓ Problemas relacionados con el rendimiento
- ✓ Añadir/Eliminar almacenamiento

- **Monitorizar el espacio libre.** Asegurarse de que se dispone de suficiente espacio para el almacenamiento debería estar en el tope de la lista de tareas diarias de un administrador de sistemas. La razón por la que la verificación frecuente de espacio disponible es tan importante es porque el espacio libre es muy dinámico; en un minuto puede haber más que suficiente espacio y al minuto siguiente casi nada. En general, hay tres razones para espacio insuficiente en disco: Uso excesivo de parte del usuario, Uso excesivo de una aplicación, Crecimiento normal en uso
- **Uso excesivo de parte de un usuario.** Algunas personas son más ordenadas que otras. Unos estarían horrorizados de ver un poco de polvo sobre sus escritorios, mientras que para otros ni siquiera pensarían dos veces sobre la colección de cajas de pizza del año pasado que tienen apilada al lado del sofá. Es lo mismo con el almacenamiento: Algunas personas son muy frugales con su almacenamiento y nunca dejan archivos innecesarios por allí. Otras personas pareciera que nunca tienen tiempo de desechar archivos que ya no necesitan. Muchas veces cuando un usuario es responsable de utilizar grandes cantidades de almacenamiento, es el segundo tipo de persona los que aparecen como responsables.
- **Manejo del uso excesivo de sus usuarios.** Esta es un área en la que un administrador de sistemas necesita reunir toda la diplomacia y habilidades interpersonales que pueda reunir. A menudo las discusiones sobre espacio en disco se pueden volver emocionales, pues la gente ve las restricciones impuestas en el espacio en disco como medidas para hacer más difícil su trabajo (o imposible), que las restricciones son ridículamente pequeñas o que sencillamente no tienen tiempo para limpiar sus archivos.

  El mejor administrador de sistemas debe tomar en cuenta muchos factores en una situación de este tipo. ¿Son las restricciones equitativas y razonables para el tipo de trabajo realizado por la persona? ¿La persona está utilizando

su espacio disponible de la forma correcta? ¿Puede ayudar a la persona de alguna forma a reducir su uso en disco (creando un CD-ROM de respaldo con todos los correos electrónicos con más de un año de antigüedad, por ejemplo)? Su trabajo durante esta conversación es intentar descubrir si este es el caso, a la vez que se asegura que alguien que realmente no tiene necesidad de tanto espacio haga su trabajo de limpieza.

En cualquier caso, lo que hay que hacer es mantener la conversación a un nivel profesional. Trate de resolver los problemas del usuario de una forma profesional ("Entiendo que esté muy ocupado, pero todos en su departamento tienen la misma responsabilidad de no desperdiciar espacio, y su utilización promedio es la mitad de la suya.") a la vez que lleva la conversación hacia el punto. El administrador de sistemas debe asegurarse de ofrecer asistencia si la falta de conocimiento/experiencia parece ser un problema. Enfocar esta situación de una manera consciente pero firme es a menudo mucho mejor que utilizar su autoridad como administrador de sistemas para lograr un resultado.

- **Uso excesivo de parte de una aplicación.** Algunas veces una aplicación es responsable por uso excesivo. Las razones para esto pueden variar, pero pueden incluir:
  - ✓ Mejoras en la funcionalidad de la aplicación que requieren mayor almacenamiento.
  - ✓ Un incremento en el número de usuarios usando la aplicación.
  - ✓ La aplicación falla en limpiar las cosas luego de su ejecución, dejando archivos temporales que ya no se necesitan en el disco.
  - ✓ La aplicación tiene problemas y el fallo que está causando esto utiliza más espacio del que debería

  Su tarea es determinar cuáles de estas razones de la lista aplican a su situación. Tener presente el estado de las aplicaciones utilizadas en su centro de datos debería ayudarle a eliminar varias de estas razones, así como también su conocimiento de los hábitos de procesamiento de sus usuarios. Lo que queda por hacer es un poco de trabajo de detective para ver donde

ha ido a parar el almacenamiento. Esto debería reducir el campo substancialmente.

En este punto debe tomar los pasos apropiados, bien sea la adición de almacenamiento para soportar la aplicación, ponerse en contacto con los desarrolladores de la aplicación para discutir sus características de manejo de archivos o escribir scripts para limpiar las cosas de la aplicación.

- **Crecimiento normal en uso.** La mayoría de las organizaciones experimentan algún nivel de crecimiento a largo plazo. Debido a esto, es normal esperar que la utilización del almacenamiento se incremente a un ritmo similar. En casi todos los casos, la supervisión contínua puede revelar la tasa promedio de utilización del almacenamiento en su organización; esta tasa puede ser usada posteriormente para determinar el tiempo en el cual se debería obtener almacenamiento adicional antes de que su espacio libre se termine.

  Si se encuentra en la posición de que repentinamente se le acaba el espacio libre debido a un crecimiento normal, entonces usted no ha estado haciendo su trabajo como debería ser.

  Sin embargo, algunas veces pueden surgir repentinamente grandes demandas de espacio adicional. Quizás su organización se haya combinado con otra, necesitando cambios rápidos en la infraestructura de IT (y por lo tanto, almacenamiento). Un nuevo proyecto de alta prioridad puede haber nacido literalmente de la noche a la mañana. Cambios a una aplicación existente pueden producir un gran incremento en las necesidades de almacenamiento.

  No importa cuál sea la razón, habrá ocasiones en que lo tomen por sorpresa. Para planear estas situaciones, trate de configurar su arquitectura de almacenamiento para un máximo de flexibilidad. El tener espacio de almacenamiento adicional a mano (si es posible) puede aliviar el impacto de estos eventos espontáneos.

- **Problemas de cuotas de usuarios.** Muchas veces cuando la gente piensa sobre cuotas de disco es para usarlas de manera de forzar a los usuarios a que mantengan limpios sus directorios. Aunque hay sitios donde este puede ser el caso, también ayuda a ver el problema de espacio en disco desde otra perspectiva. ¿Qué hay de las aplicaciones que, por una razón o la otra, consumen demasiado espacio en disco? Se sabe de aplicaciones que fallan de una forma tal en que consumen todo el espacio disponible. En estos casos, las cuotas de disco le pueden ayudar a limitar el daño causado por tales aplicaciones erráticas, forzándolas a detenerse *antes* de consumir todo el espacio en el disco.

  La parte más difícil de implementar y manejar cuotas de disco está relacionada con los límites mismos. ¿Cuál debería ser? Un enfoque simplístico sería dividir el espacio en disco por el número de usuarios y/o grupos que lo utilizan y utilizar el número resultante como la cuota por usuario. Por ejemplo, si el sistema tiene una unidad de disco de 100GB y 20 usuarios, cada usuario tendría una cuota de 5GB. De esta forma, cada usuario tendrá garantizado 5GB(aunque en este punto el disco estaría a un 100%).

  Para aquellos sistemas operativos que lo soportan, las cuotas temporales se podrían configurar un poco más altas digamos 7.5GB, dejando la cuota permanente en 5GB. Esto tiene el beneficio de permitir a los usuarios consumir de forma permanente solamente el porcentaje de disco que les corresponde, pero a la vez otorgando un poco de flexibilidad cuando el usuario alcanza (y excede) su límite. Cuando se utilicen cuotas de esta forma, usted en realidad está comprometiendo su disco más allá de su espacio disponible. La cuota temporal es 7.5GB. Si todos sus 20 usuarios exceden su cuota permanente al mismo tiempo e intenta acercarse a su cuota temporal, esos 100GB de disco deberían en realidad ser 150GB para poder permitir a todos alcanzar su cuota temporal al mismo tiempo.

  No obstante, en práctica nadie excede su cuota permanente al mismo tiempo, haciendo que este sea un enfoque aceptable. Por supuesto, la selección de

las cuotas permanentes y temporales depende del administrador del sistema, pues cada sitio y comunidad de usuarios es diferente.

- **Problemas relacionados a archivos.** Los administradores de sistemas a menudo tienen que tratar con problemas relacionados a los archivos. Estos problemas incluyen: acceso a archivos y compartir archivos.

Los aspectos descritos deben ser tomados en cuenta por todo administrador de sistemas, para de esta manera responder ante las distintas situaciones apropiadamente. Además, los siguientes puntos deben también ser tomados en cuenta ya que dependerán del tipo de sistemas operativo que estemos administrando:

- La administración del servicio de directorio.
- El control y seguimiento de los procesos del sistema.
- La gestión de la automatización de tareas del sistema.
- La administración de forma remota del sistema operativo en red.
- La administración de servidores de impresión.
- La realización de tareas de integración de sistemas operativos libres y propietarios.
- La utilización de lenguajes de scripting en sistemas operativos libres y propietarios para la administración de servicios del sistema operativo.

1.4 Funciones del administrador

Un sistema informático precisa de una planificación, configuración y atención continuada para garantizar que el sistema es fiable, eficiente y seguro. El sistema informático debe tener una o más personas designadas como administradores para gestionarlo y ver su rendimiento. El administrador del sistema tiene la responsabilidad de asegurar su adecuado funcionamiento, de saber a quién poder llamar si no se pueden resolver los problemas internamente, y de saber cómo proporcionar recursos hardware y software a los usuarios.

Las tareas y responsabilidades de los administradores de sistemas varían dependiendo del tamaño del sistema informático. En sistemas grandes las tareas de administración pueden dividirse entre varias personas. Por otro lado, algunos sistemas pequeños tan solo necesitan un administrador.

El administrador del sistema cumple un papel muy importante en la empresa, ya que debe garantizar el correcto funcionamiento del sistema informático. Además, dada la responsabilidad y el tipo de información con el que trabaja, el administrador se convierte en una persona de confianza dentro de la empresa.

La descripción exacta del trabajo del administrador del sistema operativo depende frecuentemente de cada organización. Un administrador del sistema puede encontrarse envuelto en una amplia variedad de actividades, desde establecer normas para instalar software a configurar los routers. Sin embargo, hay una serie de tareas que todos los administradores tienen que gestionar:

- **Instalación, desinstalación y configuración de software.** Instalar y configurar el sistema operativo, servicios y aplicaciones necesarios para que el servidor trabaje de forma correcta. También de ser necesario realizar la desinstalación de software y aplicaciones.
- **Instalación, desinstalación y configuración de hardware.** Instalar, configurar dispositivos como impresoras, terminales, módems, unidades de cinta, etc, y de ser necesario realizar la desinstalación de hardwares defectuosos o desfasados.
- **Actualizar el sistema operativo, las aplicaciones, los controladores, etc.** La mayoría de los sistemas operativos distribuyen las actualizaciones de los productos que forman parte del sistema.
- **Control de procesos y servicios.** En el sistema operativo se ejecutan procesos que consumen recursos, cuando un proceso tiene un comportamiento normal, consume recursos y los libera. El problema puede darse cuando un proceso intenta acceder a recursos que no hay o que están prohibidos, hay que vigilar que esta tarea se realice correctamente, si no, puede causar problemas en el sistema.

- **Crear tareas programadas.** Hay muchas tareas que se tienen que realizar en el sistema y que no tenemos que estar delante del ordenador para realizarlas, la solución es programarlas para que se ejecuten en un instante del tiempo.
- **Gestión de almacenamiento.** Cualquier dispositivo de almacenamiento como son los discos, los dispositivos usb, deben ser gestionados, ya sea borrar datos, dar formato, particionar, redimensionar, etc.
- **Instalación y configuración la red.** Instalar, configurar y realizar un mantenimiento de la red para permitir que los equipos se comuniquen correctamente.
- **Administración de usuarios**. Crear usuarios, dar de alta o baja usuarios, modificar sus características y privilegios, etc.
- **Formación y asesoramiento de los usuarios.** Proporcionar directa o indirectamente formación a los usuarios de modo que puedan utilizar el sistema de forma efectiva y eficiente.
- **Inicio y apagado del sistema.** Iniciar y apagar el sistema de un modo ordenado para evitar inconsistencias en el sistema de ficheros.
- **Registro de los cambios del sistema**. Registrar cualquier actividad significativa relacionada con al sistema.
- **Realización de copias de seguridad.** Establecer una correcta política de seguridad que permita restablecer el sistema en cualquier momento.
- **Seguridad del sistema**. Evitar que los usuarios interfieran unos con otros a través de acciones accidentales o deliberadas,
- **Reparación del sistema**: Cuando hay un fallo en el sistema operativo o en algún componente hardware, el sistema se tiene que poder recuperar.
- **Rendimiento del sistema**: Para valorar el funcionamiento de un sistema es conveniente controlar los recursos y monitorear el rendimiento que tienen.

ACTIVIDAD

Caso de Estudio

La empresa X decidió mejorar el rendimiento y estabilidad de sus sistemas, por ende, ha sido contratado un administrador de sistemas operativos.

La situación actual de la empresa X es:

- La empresa cuenta con dos sucursales, conectadas en red.
- Los usuarios por cada sucursal es de 30, divididos en 4 departamentos.
- No cuentan con asignación de grupos, ni permisos establecidos.
- No se cuenta con disposiciones para la seguridad ni respaldo de los datos.
- Sólo se cuenta con 2 impresoras por sucursal.
- El hardware de la empresa data entre 8 a 5 años de utilización permanente.
- Existen 2 diferentes sistemas, uno para la parte operativa y otro para la parte de contabilidad o finanzas.
- Las aplicaciones instaladas en los equipos no cuentan con licencias actualizadas y no existe control alguno para su instalación.
- Todos los usuarios tienen acceso a la red y descargan todo tipo de documentos de internet.

Como nuevo administrador encargado se le pide mejorar el rendimiento, minimizar los errores y las fallas de los sistemas y establecer políticas para los usuarios.

Se le asigna un cómodo presupuesto para la compra de hardware y software.

Tome en cuenta la situación actual de la empresa y presente solución para cada una de esas situaciones, detallando paso a paso y justificando las medidas a implementar.

CAPÍTULO II. ADMINISTRACIÓN DE USUARIOS Y GRUPOS

Objetivos:

- Generar información relevante que detalle la creación y administración de los usuarios del sistema.
- Resaltar la importancia de una adecuada administración de contraseñas de acceso, que podrían afectar la seguridad de todos los sistemas.
- Ejecutar la asignación de perfiles y compartición de archivos, tomando en cuenta las características del sistema.

¿De qué trata esta sesión de aprendizaje?

En esta sesión de aprendizaje se presentan aspectos fundamentales de todo sistema, como lo es, la administración de usuarios. Se verá la creación de usuarios, grupos, asignación de perfiles y la delicada tarea de manipulación de contraseñas.

2. Administración de usuarios y grupos

En informática, se denomina usuario a cada una de las personas que utilizan un sistema informático. Se dice que los sistemas operativos son multiusuarios.

La seguridad informática se basa en la administración efectiva de los permisos de acceso a los recursos informáticos.

La administración de *cuentas de usuario* y *grupos* es una parte esencial de la administración de sistemas dentro de una organización. Pero para hacer esto efectivamente, un buen administrador de sistemas primero debe entender lo que son las cuentas de usuario y los grupos y cómo funcionan.

La razón principal para las cuentas de usuario es verificar la identidad de cada individuo utilizando un computador. Una razón secundaria (pero aún importante) es la de permitir la utilización personalizada de recursos y privilegios de acceso.

Tipos de usuarios:

- **Root o superusuario.** Tiene control total sobre los recursos del sistema. Pero, por ejemplo en Ubuntu y Android, la cuenta Root viene desactivada por defecto.
- **Administrador.** Puede gestionar y configurar todos los recursos hardware (instalar periféricos,...) y software (crear usuarios, asignar permisos,...).
- **Estándar.** Tiene acceso al uso de aplicaciones, a documentos privados y a los archivos compartidos por otros usuarios. Puede llevar a cabo modificaciones en sus preferencias personales pero no en la configuración del sistema.
- **Invitado.** Usuario que tiene restricciones por cuestiones de seguridad, por lo que solamente puede hacer tareas limitadas.

2.1 Crear, añadir, modificar, eliminar usuarios

Las cuentas de usuario son el modo habitual de personalizar el acceso a los sistemas. Así, toda persona que utilice el sistema con regularidad debe tener una cuenta de acceso.

Para que el control de este acceso sea suficientemente bueno, las cuentas deben ser personales, es decir, dos usuarios no deben compartir la misma cuenta

La cuenta proporciona el acceso a la red y lleva asociadas todas las características y propiedades del usuario útiles en las labores de administración. Las cuentas de usuario suelen tener parámetros semejantes a los que a continuación se describen, aunque cada sistema operativo de red tiene los suyos propios

- **Nombre de usuario.** Es el nombre único atribuido al usuario y que utiliza para identificarse en la red. Suele ser una cadena de caracteres corta (entre uno y 16 caracteres, normalmente).
- **Contraseña.** Es la cadena de caracteres que codifica una clave secreta de acceso a la red para cada usuario. La contraseña va ligada al nombre de usuario. Proporciona la llave que protege los datos persona- les del usuario que la posee
- **Nombre completo del usuario.** Es una cadena de caracteres con el nombre completo del usuario. El nombre de usuario suele ser una abreviatura del nombre completo. En este campo se permite un número mayor de caracteres, incluyendo espacios en blanco, para identificar totalmente al usuario. Algunos examinadores de red muestran este nombre al solicitar una inspección de la red.
- **Horario permitido de acceso a la red.** Es un campo que describe las horas y los días en que el usuario tiene acceso a la red. En cualquier otro tiempo el usuario no puede presentarse en la red o es forzado a abandonarla. Por defecto, los sistemas operativos de red permiten el acceso de los usuarios cualquier día a cualquier hora
- **Estaciones de inicio de sesión.** Describe el nombre de los equipos desde los que el usuario puede presentarse en la red
- **Caducidad.** Describe la fecha en que la cuenta expirará. Es útil para cuentas de usuarios que sólo requieren accesos por periodos de tiempo concretos. Al desactivarse la cuenta, se impide que otros posibles usuarios (intrusos) se apropien indebidamente de ella y, por tanto, protegen y descargan al servidor de accesos indebidos o indeseados
- **Directorio particular.** Es el lugar físico dentro del sistema de ficheros de la red en donde el usuario puede guardar sus datos. Al presentarse en la red,

el sistema operativo le posiciona en su directorio particular o le concede acceso al mismo.

- **Archivos de inicio de sesión.** Permiten configurar un conjunto de comandos que se ejecutarán automáticamente al inicio de la sesión de red. Están ligados a cada cuenta de usuario, aunque se permite que varios usuarios compartan el archivo de inicio.
- **Otros parámetros.** Algunos sistemas operativos permiten configurar otros parámetros como son los perfiles de usuario, la cantidad de disco de que dispondrá cada usuario, disponibilidad de memoria central, tiempo de CPU, capacidad de entrada/salida, etc. Estos parámetros tienen una especial importancia en grandes sistemas multiusuario.

Añadir usuarios

Cuando se añade un usuario hay varios pasos a seguir. Primero, se le debe crear una entrada en /etc/passwd (en Linux), con un nombre de usuario y UID únicos. Se debe especificar el GID, nombre completo y resto de información. Se debe crear el directorio inicial, y poner los permisos en el directorio para que el usuario sea el dueño. Se deben suministrar ficheros de comandos de inicialización en el nuevo directorio y se debe hacer alguna otra configuración del sistema (por ejemplo, preparar un buzón para el correo electrónico entrante para el nuevo usuario).

Aunque no es difícil el añadir usuarios a mano, cuando se está ejecutando un sistema con muchos usuarios, es fácil el olvidarse de algo. La manera más simple de añadir usuarios es utilizar un programa interactivo que vaya preguntando por la información necesaria y actualice todos los ficheros del sistema automáticamente. El nombre de este programa es useradd o adduser dependiendo del software que esté instalado.

Modificar usuario

Después de que haya creado un usuario, puede necesitar cambiar algún atributo de dicho usuario, como puede ser el directorio inicial o la clave. La forma más simple de hacer esto es cambiar los valores directamente en /etc/passwd. Para poner clave a un usuario, utilice el comando passwd.

Por ejemplo, # passwd Larry cambiará la clave de larry. Sólo root puede cambiar la clave de otro usuario de ésta forma. Los usuarios pueden cambiar su propia clave con passwd también. En algunos sistemas, los comandos chfn y chsh están disponibles, permitiendo a los usuarios el cambiar sus atributos de nombre completo e intérprete de conexión. Si no, deben pedir al administrador de sistemas que los cambie por ellos.

2.2 Controlar usuarios y sus contraseñas

A la hora de seleccionar una contraseña existen una serie de recomendaciones, algunas de las cuales son tenidas en cuenta por el algoritmo de encriptación. Algunas de esas recomendaciones no pueden ser ignoradas ya que supondrían un fallo de seguridad en el sistema. Por citar algunas de las que se aplican comúnmente, están:

- Longitud mínima de 6 caracteres entre los que se recomiendan caracteres alfanuméricos y especiales.
- No se permiten palabras que aparezcan en un diccionario incorporado al sistema de encriptación.
- Se recomienda el uso de palabras no relacionadas con el usuario (nombres, fechas, etc.).
- No se permiten contraseñas que sólo contengan caracteres numéricos,
- Se recomienda el uso de caracteres y dígitos combinados en la contraseña.
- No se permiten cambios triviales sobre palabras del diccionario o derivadas.

En términos más prácticos, una contraseña proporciona una forma de probar la autenticidad de la persona que dice ser el usuario con ese nombre de usuario. La efectividad de un esquema basado en contraseñas recae en gran parte sobre varios aspectos de la contraseña:

- La confidencialidad de la contraseña
- La resistencia de adivinar la contraseña
- La resistencia de la contraseña ante un ataque de fuerza bruta

Las contraseñas que efectivamente toman en cuenta estos problemas se conocen como contraseñas *robustas*, mientras que aquellas que no, se les llama *débiles*. Es

importante para la seguridad de la organización crear contraseñas robustas, mientras más robustas sean las contraseñas, hay menos probabilidades de que estas sean descubiertas o que se adivinen. Hay dos opciones disponibles para reforzar el uso de contraseñas robustas:

- El administrador del sistema puede crear contraseñas para todos los usuarios.
- El administrador del sistema puede dejar que los usuarios creen sus propias contraseñas, a la vez que se verifica que las contraseñas sean lo suficientemente robustas.

Al crear contraseñas para todos los usuarios asegura que estas sean robustas, pero se vuelve una tarea pesada a medida que crece la organización. También incrementa el riesgo de que los usuarios escriban sus contraseñas.

Por estas razones, la mayoría de los administradores de sistemas prefieren dejar que los usuarios mismos creen sus contraseñas. Sin embargo, un buen administrador de sistemas tomará los pasos adecuados para verificar que las contraseñas sean robustas.

La necesidad de mantener secretas las contraseñas debería ser una parte arraigada en la mente de un administrador de sistemas. Sin embargo, este punto se pierde con frecuencia en muchos usuarios. De hecho, muchos usuarios ni siquiera entienden la diferencia entre nombres de usuarios y contraseñas. Dado este hecho, es de vital importancia proporcionar cierta cantidad de educación para los usuarios, para que así estos puedan entender que sus contraseñas se deberían mantener tan secretas como su sueldo.

Las contraseñas deberían ser tan difíciles de adivinar como sea posible. Una contraseña robusta es aquella que un atacante no podrá adivinar, aún si el atacante conoce bien al usuario.

Un ataque de fuerza bruta sobre una contraseña implica el intento metódico (usualmente a través de un programa conocido como *password-cracker*) de cada combinación de caracteres posible con la esperanza de que se encontrará la contraseña correcta eventualmente. Una contraseña robusta se debería construir

de manera tal que el número de contraseñas potenciales a probar sea muy grande, forzando al atacante a tomarse un largo tiempo buscando la contraseña.

Caducidad de contraseñas:

Si es posible implemente períodos de vigencia para las contraseñas. La caducidad de las contraseñas es una funcionalidad (disponible en muchos sistemas operativos) que coloca límites en el tiempo que una contraseña dada es considerada válida. Al final del tiempo de vida de la contraseña, se le pide al usuario que introduzca una nueva contraseña, que se puede utilizar hasta que, igualmente, expire.

La pregunta clave con respecto a la caducidad de las contraseñas con la que se enfrentan muchos administradores de sistemas es sobre el tiempo de vida de una contraseña: ¿Cuál es el más adecuado?

Hay dos problemas diametralmente opuestos con respecto al tiempo de vida de las contraseñas:

- Conveniencia del usuario
- Seguridad

Por un lado, un tiempo de vida de una contraseña de 99 años presentará muy pocos problemas (si es que llega a presentar alguno). Sin embargo, proporcionará muy poco en términos de mejorar la seguridad.

En el otro extremo, un tiempo de vida de una contraseña de 99 minutos será un gran inconveniente para los usuarios. Sin embargo, la seguridad mejorará en extremo.

La idea es encontrar un balance entre la conveniencia para sus usuarios y la necesidad de seguridad de su organización. Para la mayoría de las organizaciones, los tiempos de vida de las contraseñas dentro del rango de semanas - meses, son los más comunes.

2.3 Crear grupos de usuarios

Los grupos son construcciones lógicas que se pueden usar para vincular cuentas de usuario para un propósito específico.

Cuando se administran grupos dentro de una organización, es prudente identificar los datos a los que ciertos departamentos deben tener acceso, los datos que se deben negar a otros y que datos deberían ser compartidos por todos. Esto ayuda en la creación de una estructura de grupos adecuada, junto con los permisos apropiados para los datos compartidos.

Por ejemplo, asuma que el departamento de cuentas por cobrar debe mantener una lista de las cuentas morosas. Esta lista debe ser compartida con el departamento de cobros. Si el personal de cuentas por cobrar y el personal de cobranzas se colocan como miembros de un grupo llamado cuentas, esta información se puede colocar entonces en un directorio compartido (propiedad del grupo cuentas) con permisos de grupo para leer y escribir en el directorio.

Algunos de los retos con los que se encuentra un administrador de sistemas cuando crean grupos son:

¿Qué grupos crear?

¿A quién colocar en un grupo determinado?

¿Qué tipo de permisos deberían tener estos recursos compartidos?

Para estas preguntas se necesita un enfoque con sentido común. Una posibilidad es reflejar la estructura de su compañía cuando se creen grupos. Por ejemplo, si hay un departamento de finanzas, cree un grupo llamado finanzas y haga a todo el personal de finanzas parte de ese grupo. Si la información financiera es muy confidencial para toda la compañía, pero es vital para los empleados senior, entonces otorgue a estos permisos a nivel de grupo para el acceso a los directorios y los datos utilizados por el departamento de finanzas añadiéndolos al grupo.

Los permisos son reglas asociadas a objetos, como carpetas, archivos o impresoras. Definen qué usuarios pueden acceder a dichos objetos y qué pueden hacer. Las acciones que se pueden hacer en una carpeta, pueden ser leer, modificar o crear archivos en su interior. En una impresora, pueden ser eliminar tareas, configurar, etc. Los derechos son reglas que definen las acciones, que pueden hacer los usuarios, tales como, hacer una copia de seguridad de un ordenador, apagar el sistema, etc.

A cada usuario se le adjudica un permiso o privilegio, sobre los recursos del sistema. Según el permiso que tenga un usuario podrá o no acceder a un recurso, y también nos dirá qué acciones podrá o no hacer (leer, escribir, imprimir, etc.). Cada usuario puede tener un permiso o privilegio individual, pero es más práctico crear grupos de usuarios que tengan los mismos privilegios.

Políticas o directivas de grupo.

Las políticas de grupo, son un conjunto de opciones de configuración de los ordenadores y de los usuarios. Estas opciones, se guardan en los objetos de políticas de grupos (Group Policy Objects, GPOs), y están asociados a objetos del Active Directory, tales como dominios o unidades organizativas. De esta forma se puede controlar el entorno de trabajo de un grupo de usuarios, una Unidad Organizativa o un dominio, de una forma centralizada.

En las directivas de grupo, se pueden incluir parámetros de software, de seguridad, programas disponibles a los usuarios, escritorio, acceso restringido a carpetas del sistema, derechos de las cuentas de usuario, etc. Se puede evitar que los usuarios instalen software o accedan a programas o datos no autorizados, que borren datos o programas importantes, etc. Los administradores, son los que configuran estas directivas de grupo.

2.4 Asignación de permisos

La mayoría de los sistemas de archivos modernos permiten asignar permisos a los archivos para determinados usuarios y grupos de usuarios. De esta manera, se puede restringir o permitir el acceso de un determinado usuario a un archivo para su visualización de contenidos, modificación o ejecución.

El acceso de un usuario a una aplicación dada, archivo o directorio es determinado por los permisos aplicados a esa aplicación, archivo o directorio.

Además, a menudo es útil si se pueden aplicar diferentes permisos para diferentes clases de usuarios. Por ejemplo, el almacenamiento compartido debería ser capaz de prevenir la eliminación accidental (o maliciosa) de archivos de usuarios por otros usuarios, a la vez que se permite que el propietario de los archivos tenga acceso completo a los mismos.

Otro ejemplo es el acceso asignado al directorio principal de un usuario. Solamente el propietario del directorio principal debería poder crear y ver los archivos que se encuentran allí. Se debería negar el acceso a todos los otros usuarios (a menos que el usuario desee lo contrario). Esto incrementa la privacidad del usuario y previene de la posible apropiación incorrecta de archivos personales.

La asignación de permisos en una red se hace en dos fases:

- En primer lugar, se determina el permiso de acceso sobre el servicio de red; por ejemplo, se puede asignar el permiso de poderse conectar a un disco de un ordenador remoto. Esto evita que se puedan abrir unidades remotas de red sobre las que después no se tengan privilegios de acceso a los ficheros que contiene, lo que puede sobrecargar al servidor.
- En segundo lugar, deben configurarse los permisos de los ficheros y directorios (o carpetas) que contiene ese servicio de red.

  Dependiendo del sistema operativo de red, las marcas asociadas al objeto de red varían, aunque en general podemos encontrar las de lectura, escritura, ejecución, borrado, privilegio de cambio de permisos, etcétera.

En redes en las que hay que hacer coexistir sistemas operativos de red de distintos fabricantes, hay que determinar los permisos para cada uno de ellos. A veces los permisos de un tipo de sistema son trasladables fácilmente a otros sistemas, aunque normalmente no coinciden con exactitud.

2.5 Compartiendo archivos

¿Dónde los usuarios acceden a los datos compartidos?

Cuando se comparten datos entre usuarios, es un práctica común tener un servidor central (o grupo de servidores) que hacen ciertos directorios disponibles a otras máquinas en la red. De esta forma los datos son almacenados en un lugar; no es necesario sincronizar los datos entre múltiples máquinas.

Antes de asumir este enfoque, primero debe determinar cuáles son los sistemas a acceder a los datos almacenados centralmente. Al hacer esto, tome nota de los sistemas operativos utilizados por los sistemas. Esta información tiene un peso en su habilidad de implementar este enfoque, pues su servidor de almacenamiento

debe ser capaz de servir sus datos a cada uno de los sistemas operativos en uso en su organización.

Lamentablemente, una vez que los datos son compartidos entre múltiples computadores en una red, puede surgir el potencial para conflictos en la propiedad de un archivo.

Problemas globales de propiedad

El tener los datos almacenados centralmente y accesibles por múltiples computadores sobre la red tiene sus ventajas. No obstante, asuma por un momento que cada una de esas computadoras tiene una lista mantenida localmente de las cuentas de usuarios. ¿Qué tal si las listas de usuarios en cada uno de estos sistemas no son consistentes con la lista de usuarios en el servidor central? Peor aún, ¿qué pasa si la lista de usuarios en cada uno de esos sistemas no son ni siquiera consistentes unas con otras?

Mucho de esto depende sobre cómo se implementen los usuarios y los permisos de acceso en cada sistema, pero en algunos casos es posible que el usuario A en un sistema pueda ser conocido como B en otro. Esto se vuelve un verdadero problema cuando los datos son compartidos entre sistemas, pues los datos que el usuario A tiene permitido acceder desde un sistema también puede ser leído por el usuario B desde otro sistema.

Por esta razón, muchas organizaciones utilizan algún tipo de base de datos central de usuarios. Esto asegura que no haya solapamientos entre las listas de usuarios en sistemas diferentes.

Directorios principales

Otro problema que enfrentan los administradores de sistemas es si los usuarios deberían tener directorios principales centralizados.

La ventaja principal de tener un directorio principal centralizado en un servidor conectado a la red es que si un usuario se conecta a cualquier máquina en la red, podrá acceder a los archivos en su directorio principal.

La desventaja es que, si la red se cae, los usuarios a lo largo de la organización no podrán acceder a sus archivos. En algunas situaciones (tales como organizaciones que hacen gran uso de portátiles), el tener directorios principales centralizados no

es recomendable. Pero si tiene sentido para su organización, la implementación de directorios principales puede hacer la vida de un administrador mucho más fácil.

ACTIVIDAD

El administrador de usuarios en Linux

Linux aporta varias herramientas para la gestión de usuarios y grupos. Es muy importante que la administración de usuarios esté bien diseñada, especialmente si debe habilitarse posteriormente un buen sistema de permisos de acceso a ficheros, servicios y aplicaciones

La instalación del sistema operativo crea automáticamente la cuenta del administrador del sistema, que es llamada **root.** La clave de acceso de esta cuenta es generada en tiempo de instalación. Además, Linux crea algunas cuentas y grupos más en tiempo de instalación. Sin embargo, toda la gestión de usuarios debe hacerse posteriormente.

Materiales necesarios

- Un PC con Linux instalado
- Acceso a la cuenta «root» de administrador en Linux o similar
- Documentación: manual de comandos en Linux

Linuxconf es una utilidad general para la configuración del sistema operativo. Uno de los elementos que puede gestionar son los usuarios y grupos. También se pueden utilizar otras herramientas como el gestor de usuarios. El gestor de usuarios de Linux es la herramienta por excelencia y específica para la gestión de usuarios y grupos. Es una herramienta de aspecto similar al gestor de usuarios en Windows Las anteriores herramientas funcionan en un entorno gráfico. No obstante, este sistema operativo, como cualquier sistema UNIX, permite la gestión de usuarios y grupos desde la línea de comandos. Para ello se pueden utilizar comandos como

/usr/sbin/ adduser que gestionan los ficheros de cuentas y claves de acceso, que son:

- /etc/passwd (fichero de cuentas y claves de acceso).
- /etc/group (fichero de grupos).
- /etc/shadow (fichero de claves de acceso, si hemos elegido la opción *shadow passwords* en tiempo de instalación).

Realiza las siguientes tareas

- ✓ Después de familiarizarte con las utilidades de administración de usuarios y grupos, crea un sistema de cuentas para un sistema Linux.
- ✓ Prueba las distintas cuentas.
- ✓ Escribe una guía de operación básica de gestión de usuarios para administradores de sistemas Linux.
- ✓ Realiza esta misma operación sobre sistemas Windows en dos configuraciones: sobre clientes independientes de un dominio y sobre un servidor controlador de dominio en un Directorio Activo.

CAPÍTULO III. ADMINISTRACIÓN DE RECURSOS DEL SISTEMA

Objetivos:

- Conocer los recursos del sistema que deben ser gestionados o administrados para mantener el rendimiento óptimo del sistema operativo.
- Describir las medidas a tomar en cuenta en la administración de memoria, CPU, servicios de impresión y terminales, que facilitarán la labor del administrador de sistemas operativos.

¿De qué trata esta sesión de aprendizaje?

En esta sesión de aprendizaje abordaremos la tarea de un sistema operativo la cual consiste en administrar los recursos de un computador cuando hay dos o más programas que ejecutan simultáneamente y requieren usar el mismo recurso (como tiempo de CPU, memoria o impresora). Y para que esta administración de realice de la manera más eficiente posible, es necesario que el administrador de sistemas interfiera poniendo en práctica diversidad de métodos y técnicas que se estarán detallando en este capítulo.

3. Administración de recursos del sistema

Administrar los recursos del sistema (procesador, memoria, etc.) se logra realizando de manera eficiente directivas de recursos basados en configuraciones, que asignen recursos por procesos, por usuarios, o por grupos. Estas configuraciones pueden adaptarse al tipo de organización y a los recursos disponibles.

3.1 Rendimiento del Sistema y control de la CPU

A menudo conocido como poder de CPU, ciclos de CPU y otros nombres diferentes, el poder de procesamiento es la habilidad de un computador de manejar datos. El poder de procesamiento varía con la arquitectura (y la velocidad del reloj) del CPU usualmente los CPUs con velocidades del reloj más lentas y aquellos soportando tamaños de palabras más grandes tienen más poder de procesamiento que los CPUs más lentos que soportan tamaños de palabras más pequeños.

He aquí los dos principales hechos sobre el poder de procesamiento que debería tener en mente:

- El poder de procesamiento es fijo
- El poder de procesamiento no se puede almacenar

El poder de procesamiento es fijo, en el sentido de que el CPU solamente puede ir a cierta velocidad. Por ejemplo, si necesita sumar dos números (una operación que toma solamente una instrucción de máquina en la mayoría de las arquitecturas) un CPU particular lo puede hacer a una velocidad y solamente a una velocidad. Con pocas excepciones, ni siquiera es posible *reducir* la velocidad en la que el CPU procesa las instrucciones, mucho menos incrementarla.

El poder de procesamiento también es fijo en otro sentido: es finito. Esto es, hay límites para los tipos de CPUs que se pueden conectar a un computador determinado. Algunos sistemas son capaces de soportar un amplio rango de CPUs de diferentes velocidades, mientras que otros quizás no se puedan actualizar para nada.

El poder de procesamiento no se puede almacenar para usarse más tarde. En otras palabras, si un CPU puede procesar 100 millones de instrucciones en un segundo, un segundo de tiempo ocioso equivale a gastar 100 millones de instrucciones de poder de procesamiento.

Si tomamos estos hechos y los examinamos desde una perspectiva ligeramente diferente, un CPU "produce" una corriente de instrucciones ejecutadas a una rata fija. Si el CPU "produce" instrucciones ejecutadas, esto significa que otra cosa debe "consumir" las mismas. La próxima sección define a estos consumidores.

He aquí los dos principales consumidores de poder de procesamiento:

- Aplicaciones
- El sistema operativo mismo

Aplicaciones

Los consumidores más obvios de poder de procesamiento son las aplicaciones y los programas que usted desea que el computador ejecute por usted. Desde una hoja de cálculo hasta una base de datos, las aplicaciones son la razón por las que usted tiene un computador.

Un único CPU puede solamente ejecutar una cosa en un momento dado. Por lo tanto, si su aplicación se está ejecutando, el resto de las cosas en el sistema no. Lo contrario, por supuesto, también es cierto si algo diferente a su aplicación se está ejecutando, entonces su aplicación no está haciendo nada.

Pero como es que muchas aplicaciones diferentes pueden parecer que se están ejecutando al mismo tiempo bajo un sistema operativo moderno? La respuesta es que estos son sistemas operativos multiproceso. En otras palabras, estos crean la ilusión de que muchas están sucediendo simultáneamente cuando en realidad es que esto no es posible. El truco es darle a cada proceso una fracción de segundo de ejecución en el CPU antes de darle el CPU a otro proceso para la próxima fracción de segundo. Si estos *switches de contexto* ocurren con la frecuencia necesaria, se logra la ilusión de que múltiples aplicaciones se ejecutan simultáneamente.

Por supuesto, las aplicaciones hacen otras cosas que manipular datos usando el CPU. Pueden también esperar por entradas del usuario así como también realizar E/S a dispositivos tales como discos duros y visualizaciones gráficas. Cuando ocurren estos eventos, la aplicación ya no necesita el CPU. En estos momentos, el CPU se puede utilizar para otros procesos ejecutando aplicaciones sin hacer más lento la aplicación en espera.

Además, el CPU puede ser utilizado por otro consumidor de poder de procesamiento: el sistema operativo mismo.

El Sistema Operativo

Es difícil determinar cuánto poder de procesamiento consume el sistema operativo. La razón de esto es que el sistema operativo utiliza una mezcla de código a nivel de procesos y a nivel del sistema para realizar su trabajo. Mientras que, por ejemplo, es fácil utilizar un supervisor de procesos para determinar qué está haciendo un proceso ejecutando un *demonio* o *servicio*, no es tan fácil determinar cuánto poder de procesamiento el sistema operativo consume por procesamiento a nivel del sistema relacionado con E/S (lo cual usualmente se hace dentro del contexto del proceso ejecutando la E/S).

En general, es posible dividir este tipo de sobrecarga de sistema operativo en dos tipos:

- Mantenimiento del sistema operativo
- Actividades relacionadas a procesos

El mantenimiento del sistema operativo incluye actividades tales como planificación de procesos y administración de memoria, mientras que las actividades relacionadas a procesos incluyen cualquier proceso que soporta al sistema operativo mismo, tales como procesos que manejan el registro de eventos globales al sistema o el vaciado de E/S de caché.

Mejorando la escasez de CPU

Cuando no hay suficiente poder de procesamiento para la carga de trabajo, tiene dos opciones:

- Reducir la carga
- Incrementar la capacidad

Reducir la carga

Reducir la carga de CPU es algo que se puede hacer sin el gasto monetario. El truco es identificar aquellos aspectos de la carga del sistema bajo su control que se pueden reducir. Hay tres áreas en las que enfocarse:

- Reducir la sobrecarga del sistema operativo
- Reducir la sobrecarga de las aplicaciones
- Eliminar aplicaciones completas

Reducir la sobrecarga del sistema operativo

Para reducir la sobrecarga del sistema operativo, debe examinar su carga actual del sistema y determinar los aspectos del mismo que resultan en cantidades de sobrecarga excesivas. Estas áreas incluyen:

- Reducir la necesidad de planificación frecuente de procesos
- Reducir la cantidad de E/S realizada

No espere milagros, en un sistema razonablemente bien configurado, es poco probable notar un incremento del rendimiento sustancial al tratar de reducir la carga del sistema operativo. Esto se debe al hecho de que un sistema razonablemente bien configurado, por definición, resulta en una cantidad de sobrecarga mínima. Sin embargo, si su sistema está ejecutándose con poca RAM, por ejemplo, quizás pueda reducir la sobrecarga al mejorar la escasez de memoria.

Reducir la sobrecarga de aplicaciones

El reducir la sobrecarga de aplicaciones significa asegurarse de que la aplicación tiene todo lo que necesita para ejecutarse bien. Algunas aplicaciones presentan comportamientos diferentes bajo ambientes diferentes, una aplicación puede volverse muy comprometida en términos de computación cuando procesa ciertos tipos de datos, pero no para otros, por ejemplo.

El punto a tener en cuenta aquí es que debe entender las aplicaciones ejecutándose en su sistema si es que quiere que se ejecuten lo más eficientemente posible. A menudo esto implica trabajar con sus usuarios y/o los desarrolladores, para ayudar a descubrir en que formas se pueden hacer las aplicaciones para que se ejecuten más eficientemente.

Eliminar aplicaciones completas

Dependiendo de su organización, este enfoque puede que no esté disponible para usted, pues a menudo no es la responsabilidad del administrador del sistema dictar cuales aplicaciones se ejecutaran y cuáles no. Sin embargo, si puede identificar

cualquier aplicación conocida como "CPU hogs", quizás pueda influenciar para eliminarlas.

Hacer esto quizás implicará más de una persona. Los usuarios afectados definitivamente deben ser parte de este proceso; en muchos casos pueden tener el conocimiento y el poder político para llevar a cabo los cambios necesarios en las aplicaciones disponibles.

Incrementar la capacidad

Por supuesto, si no es posible reducir la demanda de poder de procesamiento, debe buscar formas de incrementar el poder de procesamiento disponible. Hacer esto cuesta dinero, pero se puede hacer.

Actualizar el CPU

El enfoque más directo es determinar si el CPU de su sistema puede ser actualizado. El primer paso es determinar si el CPU actual se puede eliminar. Algunos sistemas (principalmente portátiles) tienen CPUs que están soldados en un lugar, haciendo imposible una actualización. El resto, sin embargo, tienen CPUs en bancos, lo que hace posible su actualización, al menos en teoría.

Luego, debe investigar para determinar si existe un CPU más rápido para la configuración de su sistema. Por ejemplo, si su sistema actual tiene un CPU de 1GHz y existe una unidad de 2GHz del mismo tipo, entonces es posible hacer una actualización.

Finalmente, debe determinar la velocidad máxima del CPU soportada por su sistema. Continuando con el ejemplo anterior, aún si existe un CPU de 2GHz del mismo tipo, un intercambio simple de CPU no es una opción si su sistema solamente soporta procesadores ejecutándose a 1GHz o menos.

Si encuentra que no puede instalar un CPU más rápido en su sistema, sus opciones pueden estar limitadas a cambiar la tarjeta madre o hasta una actualización.

Sin embargo, algunas configuraciones de sistemas permiten un enfoque ligeramente diferente. En vez de reemplazar el CPU existente, porque no añadir otro?

Supervisar el rendimiento del sistema es una parte importante del mantenimiento y de la administración. Los datos de rendimiento se utilizan para:

- Comprender la carga de trabajo y el efecto que produce en los recursos del sistema.
- Observar los cambios y las tendencias en las cargas de trabajo y en el uso de los recursos. de modo que se puedan planificar las futuras actualizaciones.
- Comprobar los cambios de configuración u otros esfuerzos de ajuste mediante la supervisión de los resultados.
- Diagnosticar problemas y componentes o procesos de destino para la optimización.

3.2 Administración de la memoria

El sistema operativo es el responsable de conocer qué partes de la memoria están siendo utilizadas, definir qué procesos se cargarán en memoria cuando haya espacio disponible, asignar y reclamar espacio de memoria cuando sea necesario.
Si existe un área en la que se puede encontrar gran cantidad de estadísticas de rendimiento, esta área es la utilización de la memoria. Debido a la complejidad inherente de los sistemas operativos con memoria virtual bajo demanda de hoy día, las estadísticas de utilización de memoria son muchas y variadas, y la administración de estas es imprescindible.
Es aquí donde tiene lugar la mayoría del trabajo de un administrador de sistemas con la administración de recursos.
Los siguientes puntos representan una descripción de lo que la administración de memoria debe tener presente y que se encuentran a menudo en los funcionamientos de los sistemas:

- **Páginas dentro/fuera.** Conocer estadísticas de estos sucesos hacen posible medir el flujo de páginas desde la memoria del sistema a los dispositivos de almacenamiento masivo (usualmente unidades de disco). Altas tasas de estas estadísticas pueden representar que el sistema está corto de memoria física y que está haciendo *thrashing* o consumiendo más recursos del sistema en mover las páginas dentro y fuera de memoria que en ejecutando aplicaciones.

- **Páginas activas/inactivas** Estas estadísticas muestran qué tanto se están utilizando las páginas residentes en memoria. Una falta de páginas inactivas puede estar apuntando hacia una escasez de memoria física.
- **Páginas libres, compartidas, en memoria intermedia o en caché**. Estas estadísticas proporcionan detalles adicionales sobre las estadísticas más simples de páginas activas/inactivas. Usando estas estadísticas es posible determinar la mezcla general de utilización de memoria.
- **Intercambio dentro/fuera.** Estas estadísticas muestran el comportamiento general de la memoria de intercambio del sistema. Tasas excesivas pueden estar apuntando a una escasez de memoria física.

La supervisión exitosa de la utilización de la memoria requiere una buena comprensión de cómo funciona la memoria virtual bajo demanda de un sistema operativo.

3.3 Servicios de la impresión

No todos los usuarios de una red tienen a su disposición dispositivos de impresión en sus ordenadores locales. Las redes ofrecen la posibilidad de compartir estos dispositivos, de modo que las inversiones sean más accesibles. Las redes de área local permiten a los clientes la conexión a las impresoras disponibles en toda la red y a las que tengan derecho de acceso. Incluso es posible la conexión a impresoras que estén conectadas a redes de otros fabricantes. Por ejemplo, desde una estación Windows se puede imprimir en una impresora conectada al puerto paralelo de un servidor NetWare.

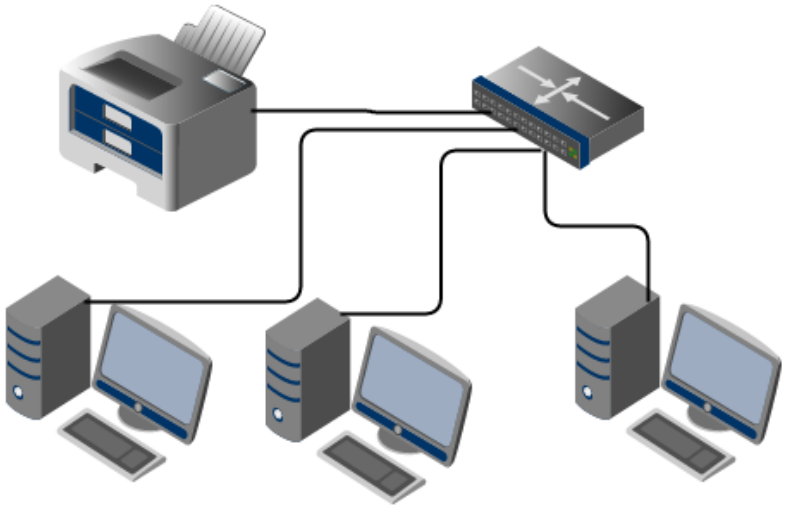

Figura 1. Ejemplo de servicio de impresión en red

La labor del administrador se simplifica cuando el sistema de impresoras está centralizado en los servidores, ya que tendrá un mayor control sobre los recursos de impresión. El administrador puede controlar los servidores de impresión, las impresoras remotas, las colas de impresoras, etcétera.

Existen servidores de impresión expresamente dedicados a este tipo de tareas, gestionando todas las tareas de impresión con arreglo a unos parámetros concretos: velocidad de impresión, calidad de impresión, privilegios, prioridades, costes, etc. Otras configuraciones, más comunes, para los servidores no dedicados se limitan a servir las impresoras que se les conectan a sus puertos de comunicaciones.

Describiremos aquí los términos y conceptos más utilizados para la descripción de un sistema de impresión en red:

- **Dispositivo de impresión.** Son los dispositivos físicos (hardware) que son capaces de producir un documento impreso. Son dispositivos de impresión las impresoras de papel, las filmadoras de película fotográfica, los plotters o trazadores gráficos, etcétera.

- **Impresoras lógicas.** Son los dispositivos lógicos (software) que nos proporciona el NOS y que conectan con el dispositivo de impresión a través de un puerto de comunicaciones.
- **Controlador de impresora.** Es un programa que convierte el documento electrónico de su formato original a un formato legible por el dispositivo de impresión. Existen varios lenguajes descriptores de páginas (PDL) legibles por los dispositivos de impresión como PCL de Hewlett-Packard, PostScript de Adobe, Interpress de Xerox, etcétera.
- **Cola de impresora.** Es un sistema gestor de los documentos que permanecen a la espera para ser impresos. En algunos sistemas operativos de red, las colas de impresora coinciden con las impresoras lógicas, siendo aquéllas una característica técnica más de éstas.
- **Administrador de trabajos en espera o spooler.** Es un sistema que gestiona las colas de impresora, es decir, es el encargado de recibir trabajos, distribuir- los entre las impresoras, descargarlos de la cola una vez impresos, avisar de la finalización de la impresión, informar de posibles errores, etcétera.

Para conseguir un rendimiento elevado y equilibrado de los dispositivos de impresión, estos parámetros deben estar correctamente configurados en el NOS. Como con cualquier otro recurso de red, también aquí son aplicables los permisos de uso y su administración remota. Para ello, es recomendable la utilización de los documentos de ayuda que proporciona el fabricante del NOS.

3.3.1 Instalación y administración

Un buen diseño del sistema de impresión redunda en una mayor eficacia del sistema, así como en un abaratamiento de los costes de instalación, al poder reducir el número de impresoras sin perder funcionalidad. Articularemos el diseño del sistema de impresión en diversas fases:

- **Elección de los dispositivos de impresión**. Deben ser elegidos de acuerdo con las necesidades de los usuarios. Es útil considerar los siguientes elementos antes de tomar las decisiones de instalación:

- ✓ Pocos dispositivos de impresión de alto rendimiento frente a muchos dispositivos de rendimiento moderado.
- ✓ Número de páginas totales que se van a imprimir y velocidad de impresión de las mismas.
- ✓ Calidad de impresión, elección de color o blanco y negro, tamaño de la página impresa, etcétera.
- ✓ Conectividad del dispositivo de impresión. Impresoras conectadas a un puerto paralelo o USB de un servidor, impresoras conectadas directamente a la red, etcétera.
- ✓ Tecnología de impresión. Las impresoras pueden ser matriciales, láser, de inyección de tinta, de sublimación, etcétera.
- ✓ Protocolos de comunicación. En el caso de las impresoras de red, hay que tener en cuenta el protocolo que utiliza para que los clientes realicen la conexión con la impresora.
- ✓ Costes de los equipamientos de impresión y de sus consumibles, costes por página impresa, etcétera.

- **Asignación de las impresoras a los equipos.** Seguidamente, hemos de distribuir las impresoras por toda la red teniendo en cuenta las características de los equipos. Se puede considerar lo siguiente:
  - ✓ El proceso de impresión consume muchos recursos de CPU; por tanto, las impresoras servidas a la red deben residir en máquinas con suficiente potencia si se prevé que la impresión va a ser frecuente.
  - ✓ Además, normalmente, cada trabajo por imprimir debe almacenarse en el disco duro del servidor de la impresora, con lo que debemos asegurarnos que tendrá suficiente espacio libre.
  - ✓ Las impresoras deben estar geográficamente distribuidas por toda la organización de acuerdo con unos criterios. Hay empresas que prefieren centralizar todas las impresoras con el fin de evitar ruidos, especialmente en el caso de impresoras matriciales o de línea, mientras que otras prefieren una distribución por departamentos o, incluso, la asignación de una impresora por cada usuario.

- **Acceso a las impresoras.** Para definir el acceso a las impresoras, hemos de considerar dos partes bien diferenciadas:
  - ✓ La asignación de impresoras lógicas a dispositivos de impresión. Pueden darse los casos de una a uno, una a varios y varias a uno. Todos los sistemas admiten la asignación uno a uno. El resto de asignaciones son posibles en función de los sistemas operativos: frecuentemente es necesario instalar software de terceras partes.
  - ✓ La asignación de los derechos de acceso para cada usuario o para cada grupo.

Algunos NOS disponen de herramientas de administración para lograr que las impresoras disparen trabajos en determinadas circunstancias. Por ejemplo, a partir de cierta hora nocturna, una impresora matricial inicia la impresión de unos recibos que han sido confeccionados y enviados a la impresora durante el día.

Del mismo modo, se pueden asignar prioridades a los diferentes trabajos, de modo que se altere el orden en que los trabajos serán seleccionados por el *spooler* para ser impresos. Además, cuando una cola atiende a varios dispositivos de impresión, el primero que quede libre recibirá el siguiente de entre todos los trabajos pendientes en esa cola.

Samba es el método más utilizado para permitir la integración entre sistemas ya que nos permite que los equipos Windows y GNU/Linux puedan compartir carpetas e impresoras entre sí. Samba es una colección de programas que hacen que Linux sea capaz de utilizar el protocolo SMB (Server Message Block) que es la base para compartir ficheros e impresoras en una red Windows. Los posibles clientes para un servidor SMB incluyen LAN Manager, Windows NT, OS/2 y otros sistemas GNU/Linux.

3.4 Administración de terminales

En las estaciones de trabajo se han de instalar y configurar todos los protocolos necesarios para la conexión a cuantos servidores necesiten los usuarios.

Por ejemplo, habrá que instalar TCP/IP si se desea hacer una conexión hacia máquinas UNIX, NetBEUI para realizar conexiones sencillas a servidores Microsoft e IPX para la conexión con servidores Novell.

Si instalamos más protocolos de los que realmente se utilizarán haremos un consumo excesivo e inútil de memoria central, así como una sobrecarga en el software de red de las estaciones, lo que ralentizará tanto los procesos informáticos como los de comunicaciones.

También hay que asegurarse de que si una aplicación tiene previsto utilizar un interfaz de aplicaciones concreto, por ejemplo, NetBIOS, debe estar instalado, ya que de lo contrario la aplicación de usuario no podrá gestionar las unidades de red remotas.

El administrador debe valorar el modo en que trabajarán los usuarios, con información local o centralizada. Podemos encontrarnos con tres tipos de configuraciones para los clientes:

- Los programas y aplicaciones están instalados en el disco duro local de la estación y no son compartidos por la red. Cada usuario tiene una copia de cada aplicación. Los datos residen también de modo habitual en el disco local, aunque es posible centralizar la información en los servidores.
- Los programas están instalados en el servidor y todos los usuarios acceden al servidor para disparar sus aplicaciones. Por tanto, se instala una única copia de las aplicaciones, lo que ahorra espacio en disco. Hay que tener en cuenta, no obstante, que no todas las aplicaciones permiten esta operativa de trabajo. Los datos de usuario pueden seguir estando distribuidos por las estaciones clientes, aunque también pueden residir en el servidor.
- Los clientes ligeros o las estaciones que no poseen disco local (o que poseyéndolo, no lo utilizan para almacenar aplicaciones o datos) y que deben arrancar remotamente a través de la red desde un servidor de sistemas operativos.

  La instalación de aplicaciones distribuidas exige la colaboración del cliente y del servidor, o entre varios servidores, para completar la aplicación. Por ejemplo, una aplicación de correo electrónico consta de una parte

denominada **cliente,** que se instala en la estación cliente, y una parte denominada **servidor,** que se instala en el servidor de correo.

3.5 Administración de módems

Los módems son objetivos de los ciberdelincuentes ya que pueden acceder a contraseñas, cuentas bancarias y números de tarjetas de crédito. Para proteger los sistemas de información de la empresa, es necesario tomar en cuenta estos consejos en la administración de estos dispositivos y de esta manera mantenerlos seguros y prevenir ataques:

1. **Cambiar las contraseñas.** Los módems suelen venir de fábrica con una contraseña pero se recomienda cambiarla. Lo primero que hay que hacer es encontrar el puerto en el que está instalado el módem.
2. **Establecer una contraseña fuerte**. Es importante elegir una contraseña que sea segura. Hay que evitar el uso de fechas, nombres o palabras que aparecen en el diccionario. Lo mejor es combinar números, letras y símbolos y que tenga al menos ocho caracteres. Otro consejo es elegir la red wifi de cifrado correcta. La más segura suele ser WPA2-PSK.
3. **Cambiar los DNS de su proveedor de internet.** Los delincuentes cibernéticos secuestran los servidores y los utilizan un período de tiempo para dirigir a los usuarios a sitios web falsos de bancos o instalar malware. La forma más fácil de prevenir este ataque es utilizando un servidor DNS.
4. **Cambia los puertos predeterminados**. Se puede configurar la red para utilizar puertos diferentes a 192.168.0.1; 192.168.1.1 o 192.168.1.100, esto hace que convertirse en víctima de un ciberataque sea más complejo.
5. **Actualizar el firmware del módem**. Actualizar el firmware de los dispositivos soluciona fallos de seguridad. Es necesario hacerlo de forma correcta porque una actualización errónea puede detener el equipo.
6. **Apagar los servicios innecesarios y configurar correctamente**. Ofrecen acceso remoto a servicios u otras tecnologías que rara vez se utilizan y se deben desactivar por seguridad:

- ✓ Administración remota y otros servicios: A veces solo se puede acceder al módem localmente (LAN). Algunos fabricantes ofrecen una función de gestión remota. Asegúrate de que el panel no es accesible a través de la web.
- ✓ La red SSID: un módem transmiten su ID públicamente. La desactivar la emisión SSID, la red no será visible y hay que introducir el nombre de la red cada vez que se conecte un nuevo dispositivo.

7. **No perder de vista webs HTTPS**. Cuando un módem o recibe un ataque y otros servidores DNS están configurados en los dispositivos, es común que se redireccione a páginas falsas maliciosas o sin conexiones "HTTPS", lo que indica la ausencia de una conexión segura (SSL).
8. **Utiliza un buen programa antimalware**. Los programas antimalware modernos protegen las conexiones poco seguras, incluso las realizadas por redes wifi extremadamente peligrosas y vulnerables.

3.6 Otros dispositivos

Administración de dispositivos extraíbles

En múltiples organizaciones los dispositivos extraíbles son un medio indispensable para el traspaso de información de forma rápida y sencilla, cargar nuevas configuraciones, actualizar el firmware de un dispositivo, etc. No obstante, si no tenemos una política rigurosa y llevamos a cabo buenas prácticas para su uso, pueden convertirse en una amenaza en vez de ayudar a prevenirlas. Por este motivo, debemos tener claro cuál es el rol de los USB dentro de SCI, sus ventajas mediante un uso correcto y mejorar sus puntos más débiles para evitar riesgos innecesarios.

Los dispositivos USB extraíbles y las unidades de memoria flash, son muy utilizados en el día a día dentro de los Sistemas de Control, por ese motivo tenemos que tener especial cuidado, ya que son uno de los principales vectores de amenaza en el ámbito de la ciberseguridad. El conflicto surge debido a que las redes industriales son bastante complejas y, además, solemos encontrar gran cantidad de dispositivos

que no se encuentran conectados a la red por cuestiones de seguridad, por lo que una de las formas más habituales de acceder a ellos es mediante USB.

Estos medios extraíbles son una forma de simplificar este procedimiento, pero a su vez, conlleva el riesgo de introducir algún malware en estos sistemas o la posibilidad de que sea un BadUSB. Por otra parte, tener una gran variedad de dispositivos de campo hace complicado, sino imposible, la gestión a todos desde una misma aplicación, y se requiere en general el uso de USB para tratar con ellos. También se debe hacer hincapié en que la vida útil de los equipos suele ser bastante larga y se combinan sistemas heredados. Por supuesto, la mayor amenaza que tienen los USB es el personal que maneja los dispositivos de control, ya que son ellos los encargados de manipular estas memorias.

Uso seguro de USB

La seguridad de los USB debería incluir controles técnicos y normativos, ya que confiar solo en las actualizaciones no será suficiente para prevenir posibles amenazas.

Además de contar con una política interna para la utilización de dispositivos USB, hay que implantar buenas prácticas que nos ayudarán a minimizar el riesgo de infección en nuestro entorno:

- Usar siempre USB corporativos que estén debidamente protegidos y con las medidas de seguridad adecuadas, almacenándolos en lugares apropiados, e informar al departamento responsable si hubiese algún incidente.
- Controlar los dispositivos externos utilizados dentro de la empresa mediante un inventariado, que incluya un identificador inequívoco para cada uno.
- No usar dispositivos personales para almacenar información referente a la empresa, en la medida de lo posible. Y si fuese necesario su uso, hacerlo teniendo la autorización de un superior o técnico, cumpliendo las políticas internas referentes al mismo, que debería incluir como mínimo un formateo, cifrado, borrado seguro de los datos y el escaneo previo.
- Siempre que sea posible, usar los dispositivos en un entorno de prueba para verificar que no contengan ninguna amenaza.

- Análisis frecuentes de los medios extraíbles mediante antivirus, por prevención.
- Borrado seguro de la información confidencial, asegurándonos de que nadie podrá recuperar esos datos.
- Seguridad de puertos USB inmediata y personalizada para redes industriales, obteniendo una mejora en la seguridad y reduciendo la infección de malware u otras amenazas.
- Actualizaciones de seguridad en curso y continuas para los USB.
- Mejor visibilidad de la utilización de USB y actividad de amenazas mediante el control de riesgos que podemos obtener, si seguimos una buena política de seguridad.
- Formación en el uso correcto de este tipo de dispositivos en las empresas a todos los empleados para que sean conscientes de las posibles amenazas, fomentar así el uso seguro y responsable y evitar los riesgos innecesarios.
- Nunca usar dispositivos de origen desconocidos que se hayan encontrado fuera o dentro de la zona de trabajo.

Aunque es cierto que los tipos de amenazas provocadas por medios USB han sido más serias de lo que se pensaba inicialmente, es inevitable que siga habiendo exposición a amenazas para los dispositivos vía USB. Sin embargo, con una política correcta y el seguimiento de unas buenas prácticas de uso de estos dispositivos, se podrá reducir la mayoría de los peligros.

ACTIVIDAD

- ✓ Crea una impresora en Windows y Linux para su conexión al puerto paralelo o USB.
- ✓ Añade permisos para que pueda imprimir algún usuario y realiza pruebas de impresión.
- ✓ Cambia algunas propiedades de la impresora y prueba los cambios.
- ✓ Asigna permisos a los distintos usuarios de la impresora y verifica que su funcionamiento es correcto.
- ✓ Sirve la impresora a la red y comprueba que desde otros clientes que se puedan conectar a la impresora se puede imprimir por ella a través de la red.
- ✓ Ahora, sobre el sistema Windows, instala el protocolo de impresión por Internet, es decir, el protocolo IPP. Comprueba que puedes gobernar la impresora desde el explorador de Internet mediante el protocolo IPP.

CAPÍTULO IV.MONITORIZACIÓN Y MANTENIMIENTO

Objetivos:

- Valorar la importancia de que el administrador del sistema mantenga frecuentemente la monitorización del rendimiento del sistema y realice oportunamente el mantenimiento de los recursos.
- Tratar la comprensión de archivos como forma de representar una determinada información empleando una menor cantidad de espacio.
- Distinguir los tipos de almacenamiento en disco.
- Preparar técnicas y herramientas para la gestión de redes y su apoyo en la administración de sistemas.
- Indagar en los métodos para realizar el respaldo y la recuperación de datos en el caso de que ocurra la perdida o borrado de estos.

¿De qué trata esta sesión de aprendizaje?

Con la fuerte expansión de las TICs en las empresas e instituciones cada vez se hace más necesario el uso de herramientas que permitan monitorizar el correcto funcionamiento de los diferentes recursos, servicios y equipos. La monitorización de sistemas es la encargada de supervisar continuamente los diferentes recursos y servicios de la empresa para garantizar el nivel de disponibilidad requerido y en caso de un posible fallo alertar a los administradores para que lo solucionen. En definitiva, el objetivo de la monitorización del sistema es garantizar que el sistema funcione correctamente y minimizar el tiempo de caída de un servicio. El objetivo de la monitorización y el mantenimiento es garantizar que el tiempo de detección de un fallo sea mínimo.

4. Monitorización y mantenimiento

La monitorización de equipos, usuarios, servicios y recursos del sistema operativo es una parte fundamental de la administración. Hay que seleccionar lo que se desea monitorizar y después, a través de los registros de sucesos, controlar los patrones de uso, los problemas de seguridad y las tendencias de tráfico. Se puede monitorizar en tiempo real el sistema, su estabilidad y rendimiento y crear alertas y registros de seguimiento, además también se puede crear bitácoras de lo que ha pasado en el sistema.

Supervisar el rendimiento del sistema es una parte importante del mantenimiento y de la administración del sistema operativo. Los datos de rendimiento se utilizan para:

- Comprender la carga de trabajo y el efecto que produce en los recursos del sistema.
- Observar los cambios y las tendencias en las cargas de trabajo y en el uso de los recursos, de modo que se puedan planificar las futuras actualizaciones.
- Comprobar los cambios de configuración u otros esfuerzos de ajuste mediante la supervisión de los resultados.
- Diagnosticar problemas y componentes o procesos de destino para la optimización.

4.1 Gestión de almacenamiento en disco

La utilización masiva de servidores de ficheros y BBDD en las redes actuales, han hecho del espacio de almacenamiento, un recurso común a los usuarios y un elemento escaso que hay que optimizar.

La gestión de almacenamiento de discos, es una utilidad del sistema para administrar los discos duros y los volúmenes o particiones que contienen. Con la administración de discos, puede crear volúmenes, formatearlos con los sistemas de archivos, inicializar discos y crear sistemas de discos tolerantes a errores.

El administrador utiliza agentes que recolectan información sobre el grado de ocupación de los discos con objeto de tomar decisiones al respecto de la redistribución de ficheros y de la adquisición de nuevos discos.

La extracción de información que realiza el agente suele ser a nivel de:

- Partición: utilización del espacio de la partición (poco nivel de detalle)
- Directorios: grado de utilización del espacio para los directorios.
- Ficheros: tamaño que ocupan los ficheros.

Al igual que con otras actividades de administración se suelen programar una serie de eventos consistente en ciertos límites que cuando son sobrepasados elevan una alarma que es comunicada al administrador a través de un mensaje en la consola, un correo electrónico o un mensaje a un móvil por ejemplo.

La tarea de recoger información, normalmente se puede hacer en background sin afectar a los procesos en ejecución, aunque también, pueden ser planificados para su posterior ejecución.

4.1.1 Discos, volúmenes, particiones

El administrador de sistemas operativos debe realizar periódicamente el chequeo del estado de los discos duro del sistema, estos estados podrían ser si un disco está en línea (disponible) o sin conexión.

- **Discos básicos y discos dinámicos**

  Los discos básicos se ajustan al esquema orientado a la partición de la organización de discos. En el caso de las actualizaciones, los discos con particiones se inicializan automáticamente como discos básicos, de modo que se pueda mantener las particiones y volúmenes creados. Los discos nuevos o vacíos pueden inicializarse como básicos o como dinámicos tras la instalación. Sin embargo, para configurar un nuevo sistema de discos tolerante a errores o para realizar cambios a los discos sin reiniciar el equipo, debe utilizar los discos dinámicos.

  Si contiene particiones primarias y extendidas con discos lógicos, los discos nuevos que se añadan al equipo que ejecute el sistema operativo serán discos básicos.

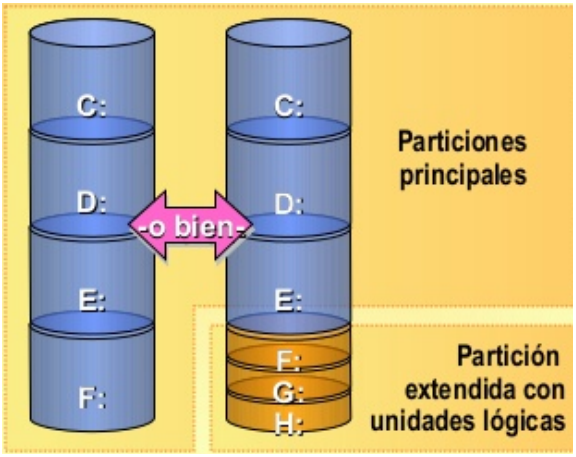

Figura 2: Los discos básicos pueden contener 4 particiones principales o 3 particiones principales y una partición extendida

El número de particiones que puede crear en un disco básico depende del estilo de partición del disco:

- ✓ En los discos de registro de inicio maestro (MBR), puede crear hasta cuatro particiones primarias por disco, o bien puede crear hasta tres particiones primarias y una partición extendida. Dentro de la partición extendida, puede crear un número ilimitado de unidades lógicas.
- ✓ En Windows Server se pueden crear, eliminar y formatear particiones sin tener que reiniciar el equipo para que se activen los cambios.

Un disco dinámico es un disco físico que contiene volúmenes dinámicos creados con Administración de discos. Los discos dinámicos no pueden contener particiones ni unidades lógicas, y no se puede tener acceso a los mismos desde MS-DOS.

Hay cinco tipos de volúmenes dinámicos: simple, distribuido, seccionado, reflejado y RAID-5. Los volúmenes reflejados y RAID-5 son tolerantes a errores. El almacenamiento dinámico tiene ventajas importantes:

- ✓ Los volúmenes se pueden ampliar para incluir espacios no contiguos de discos disponibles.
- ✓ No hay límites en el número de volúmenes que se pueden crear por disco.

- ✓ La información de la configuración del disco se almacena en el disco. Esta información se replica al resto de discos dinámicos para que si un disco falla no obstruya en el acceso a datos de los otros discos.

El almacenamiento dinámico ofrece los siguientes tipos de volúmenes:

- ✓ Un volumen simple contiene el espacio de disco de un sólo disco dinámico. Puede abarcar una sola región o varias regiones del mismo disco vinculadas entre sí. Si el volumen simple no es un volumen del sistema ni un volumen de inicio, se puede extender en el mismo disco o en discos adicionales. Si lo extiende en varios discos se convierte en un volumen distribuido.
- ✓ Los volúmenes distribuidos contienen espacio en disco en más de un disco físico. Se puede aumentar el tamaño de un volumen distribuido si se extiende en discos dinámicos adicionales. No son tolerantes a fallos pero se pueden reflejar.
- ✓ Volúmenes seccionados almacenan datos en bandas de dos o más discos físicos. Los datos de un volumen seccionado son asignados de forma alternativa y equitativa (en bandas) en los discos. Estos volúmenes ofrecen mejor rendimiento de todos los disponibles en Windows, pero no son tolerantes a fallos. No se pueden reflejar ni ampliar.
- ✓ Los volúmenes en espejo o reflejado son dos copias idénticas de un volumen simple, cada una en un disco duro diferente. Proporcionan tolerancia a fallos.
- ✓ RAID-5 es un volumen de paridades distribuida con tolerancia a fallos. RAID-5 requiere un mínimo de 3 discos duros.

Tanto si el disco dinámico utiliza el estilo de partición con registro de inicio maestro (MBR) como si usa una tabla de particiones GUID (GPT), es posible crear hasta 2.000 volúmenes dinámicos, aunque el número recomendado es de 32 o menos volúmenes dinámicos.

Un disco duro puede ser o básico o dinámico, no pudiéndose combinar los dos tipos de almacenamiento en un disco. Se puede combinar el tipo

de almacenamiento en discos diferentes. Tanto para los discos básicos como para los dinámicos, puede:

- ✓ Comprobar las propiedades de disco como la capacidad, el espacio disponible en disco y el estado actual.
- ✓ Ver las propiedades de partición y volumen como el tamaño, la asignación de letras de unidad, etiquetas, tipos y sistema de archivos.
- ✓ Establecer asignaciones de letras de unidad para volúmenes o particiones.
- ✓ Establecer las medidas de seguridad y uso compartido de disco para un volumen o partición.
- ✓ Crear y eliminar particiones principales y particiones extendidas

En Windows Server, de manera predeterminada, los discos que se hayan detectado recientemente se conectan con acceso de lectura y escritura, salvo que estén en un bus compartido (por ejemplo, SCSI, iSCSI, Serial Attached SCSI o Fibre Channel). Los discos de un bus compartido están sin conexión la primera vez que se detectan. Si un disco está sin conexión, debes conectarlo para poder inicializarlo o crear volúmenes en él.

Un disco básico es un disco físico que incluye particiones principales, particiones extendidas o unidades lógicas. Las particiones y unidades lógicas en los discos básicos se conocen como volúmenes básicos. Solo puedes crear volúmenes básicos en los discos básicos.

Puedes agregar más espacio a las particiones existentes principales y unidades lógicas ampliándolas con espacio sin asignar, contiguo y adyacente en el mismo disco.

- **Volúmenes y particiones**

  En un disco dinámico, el almacenamiento se divide en volúmenes en vez de en particiones. Puede actualizar el almacenamiento básico al almacenamiento dinámico en cualquier momento. Cuando actualiza al

almacenamiento dinámico, las particiones existentes se convierten en volúmenes como se muestra en la siguiente tabla:

Tabla 1: Comparativa de organización de discos básicos y discos dinámicos

Organización en discos básicos	Organización en discos dinámicos
Partición	Volumen
Particiones de inicio y de sistema	Volúmenes del sistema y de inicio
Partición activa	Volumen activo
Partición extendida	Volúmenes y espacio sin asignar
Unidad lógica	Volumen simple
Conjunto de volúmenes	Volumen distribuido
Conjunto de bandas	Volumen con bandas
Conjunto de espejos	Volumen reflejado

En un disco básico, la partición hace que un disco duro, o una parte de él, pueda ser utilizado como medio de almacenamiento (también se les puede denominar volúmenes).

Constituyen la manera en que se divide el diseño físico, de forma que cada una de las particiones funciona como si fuera una unidad separada.

Las particiones pueden ser de dos tipos:

- **Particiones primarias.** Son reconocidas por la BIOS del ordenador como capaces de iniciar el sistema operativo desde ellas. Para ello disponen de un sector de arranque (BOOT SECTOR), que es el que se encarga de cargar el sistema operativo, y una de las particiones primarias debe estar declarada como activa.
- **Particiones secundarias o extendidas.** Se forman en las áreas del disco duro que no tienen particiones primarias y que están contiguas.
    - ✓ Las particiones extendidas deben estar configuradas en unidades lógicas para que se pueda almacenar información.
    - ✓ Las particiones secundarias se pueden dividir en una o varias unidades lógicas (puede haber un número ilimitado de unidades lógicas en un disco) que son partes más pequeñas de la partición.

Con un programa de inicialización adecuado se puede seleccionar entre diferentes sistemas operativos para iniciar el que se desee. Cada uno de ellos deberá estar en

su propia partición y el programa de inicialización pondrá la partición seleccionada como activa.

Las particiones deben estar formateadas para establecer letras de unidades que van desde la C: en adelante.

En un disco dinámico, **un volumen** es una parte de un disco físico que funciona igual que una unidad separada. Es equivalente a las particiones primarias de los discos básicos.

4.1.2 Compresión de archivos

La compresión de datos o archivos es la reducción del volumen de datos tratables para representar una determinada información empleando una menor cantidad de espacio. Al acto de compresión de datos se denomina *compresión*, y al contrario *descompresión*.

El objetivo de la compresión es siempre reducir el tamaño de la información, intentando que esta reducción de tamaño no afecte al contenido. No obstante, la reducción de datos puede afectar o no a la calidad de la información:

- ✓ **Compresión sin pérdida:** los datos antes y después de comprimirlos son exactos en la compresión sin pérdida. En el caso de la compresión sin pérdida una mayor compresión solo implica más tiempo de proceso. Se utiliza principalmente en la compresión de texto.
- ✓ **Un algoritmo de compresión con pérdida** puede eliminar datos para reducir aún más el tamaño, con lo que se suele reducir la calidad. Hay que tener en cuenta que una vez realizada la compresión, no se puede obtener la señal original, aunque sí una aproximación cuya semejanza con la original dependerá del tipo de compresión. Se utiliza principalmente en la compresión de imágenes, videos y sonidos.

La compresión de archivos y carpetas permite almacenar grandes cantidades de datos en menos espacio. Los archivos y carpetas que se copian o mueven pueden mantener su estado de compresión o asumir el estado de compresión de la carpeta de destino.

Cada archivo y carpeta en un volumen NTFS tiene un estado de compresión, está comprimido o sin comprimir.

El estado de compresión de una carpeta no refleja necesariamente el estado de compresión de los archivos y subcarpetas que contiene. Los archivos sin comprimir pueden estar en una carpeta comprimida y los archivos comprimidos pueden estar en una carpeta con estado sin comprimir.

Para cambiar el estado de compresión de un archivo de una carpeta se debe disponer de permisos de escritura para el archivo o carpeta.

No se pueden comprimir archivos o carpetas cifradas.

La asignación de espacio al copiar o mover un archivo o carpeta se basa en el tamaño sin comprimir.

4.2 Gestión de las comunicaciones en la red

En la actualidad la dependencia de las tecnologías de información y comunicaciones en todos los ámbitos de la vida cotidiana es incuestionable.

La gestión en las comunicaciones trata sobre un conjunto de técnicas tendientes a mantener una red operativa, eficiente, segura, constantemente monitorizada y con una planeación adecuada, siempre manteniendo todo documentado de manera correcta.

Los administradores de red son las personas que se encargan de administrar y mantener las redes tanto en software como en hardware, algo así como el administrador de sistemas, pero en redes!

Los administradores, analistas y especialistas de red, concentran la mayoría de sus esfuerzos en diseñar y mantener segura la red, buscando siempre la depuración de elementos que puedan dañar la red y resolviendo problemas relacionados que se presenten en ella.

Según el modelo OSI, se definen 5 funciones básicas al momento de gestionar las comunicaciones:

- Seguridad: El administrador provee mecanismos para asegurar el control de accesos, manejo de claves y confidencialidad de las mismas.

- Comportamiento: Se encarga de balancear la red a niveles aceptables para su buen uso.
- Contabilidad: El cual permite el establecimiento de cargos a usuarios por uso de recursos de la red.
- Fallas: Se basa en la detección, aislamiento y corrección de fallas.
- Configuración: Se basa en las funciones de monitoreo y mantenimiento.

Derivando de estas características principales, también se dan las funciones de:

- Dar servicio de soporte a todos los usuarios de la red, cuando estos lo necesiten.
- Instalación y configuración de redes y sus respectivos equipos.
- Crear y Administrar todas las cuentas de usuarios que hacen uso de la red.
- Encargado del buen funcionamiento de todos los recursos de la red.
- Asegurar el uso eficiente y oportuno de la red.
- Documentar y administrar los programas instalados.
- Hacer seguridad preventiva y correctiva.
- Asegurar el alcance de los objetivos de calidad y servicio.
- Efectuar auditorias y análisis constantes de la red.

Elementos involucrados en la gestión de comunicaciones:

- Objetos: son los elementos de bajo nivel, incluyen los aparatos administrados.
- Agentes: Puede ser un solo programa o un conjunto de programas que recopilan información de todo lo que sucede en la red en un solo nodo central. El agente se encarga de entregar información al administrador sobre: notificación de problemas, datos de diagnóstico, característica e identificación del nodo.
- Administrador del sistema: Es un conjunto de softwares ubicados en un punto central, que monitorizan las redes cuando es necesaria una acción o cuando el administrador solicita alguna información.
- Administración de fallas: maneja las condiciones de error en todos los componentes de la red, en las siguientes fases:

- ✓ Detección de fallas.
- ✓ Diagnóstico del problema.
- ✓ Darle la vuelta al problema y recuperación.
- ✓ Resolución.
- ✓ Seguimiento y control.

- Servicios de contabilidad: Esta operación concierne a proveer datos concernientes al cargo por uso de la red; entre los datos proporcionados tenemos: tiempo de conexión y terminación, número de mensajes transmitidos y recibidos, nombre del punto de acceso al servicio, razón por la que terminó la conexión.
- Administración del comportamiento: Uno de los principales objetivos es mantener la red operativa al 100%, lo que incluye que puede establecer reglas sobre la cantidad de paquetes que se transmiten por segundo, tiempo de respuestas y disponibilidad.

4.2.1 Protocolos

Una vez establecida una comunicación segura puede ser necesaria la identificación de una de las partes como cliente y en la otra parte como servidor. Para ello se pueden utilizar diferentes algoritmos, protocolos y sistemas. Entre estos podemos mencionar:

- **Kerberos.** es un protocolo de autenticación de partes cliente-servidor que permite autenticar ambas partes sobre un medio inseguro. Se basa en cifrado simétrico (DES) y un tercero en quien confían ambas partes (KDC *Key Distribution Center*). Este tercero provee las funciones de autenticación (AS: *Authentication Server*) y despacho de etiquetas (TGS: *Ticket Granting Server*). Todas las partes deben autenticarse en el AS. Algunas extensiones de Kerberos permiten el uso de PKI. La version 5, vigente, permite el uso de AES en vez de DES.

  Todos los equipos gestionados por un servidor forman un dominio o territorio Kerberos (*realm*).

- **SSL y TLS (*Transport Layer Security*)** es un protocolo estándar basado en SSL (*Secure Sockets Layer*), desarrollado por Netscape. TLS permite establecer comunicaciones seguras punto-a-punto por encima de la capa de transporte de la red (generalmente TCP/IP). TLS otorga autenticación (mediante PKI), confidencialidad e integridad. La autenticación puede ser unilateral (por ejemplo en un entorno web cliente-servidor) o bilateral, ya sea utilizando PKI, TLS-PSK o SRP.

  Durante el inicio de la comunicación los extremos negocian el algoritmo de cifrado simétrico a utilizar, realizan el intercambio (o acuerdo) de clave y acuerdan los algoritmos de firma a utilizar. Una vez establecida la comunicación se utiliza el algoritmo de clave simétrica (con la clave acordada) para cifrar la comunicación y el algoritmo de firma para generar los códigos de autenticación de los mensajes (MAC: *Message Authentication Codes* o kHMAC). Los algoritmos más utilizados en TLS son:

  - ✓ Para intercambio de claves: RSA, Diffie-Hellman, ECDH, SRP, PSK
  - ✓ Para autenticación de las partes: RSA, DSA, ECDSA
  - ✓ Para cifrado: Triple DES, AES, IDEA
  - ✓ Para firma de mensajes: HMAC-MD5 (SSLv2 en desuso) o HMAC-SHA (SSLv3).
- **IKE. IKE (*Internet Key Exchange*) o IKEv2** permite la creación de conexiones de seguridad que utiliza DH para el intercambio de claves y PSK, PKI o Kerberos para la autenticación de las partes. Permite negociar el cifrado simétrico y la firma de mensajes. IKE funciona sobre UDP y, entre otros, es utilizado por ISAKMP y EAP-IKE.
- **ISAKMP (*Internet Security Association and Key Management Protocol*).** Es un esquema utilizado en IPSec para establecer comunicaciones seguras (crear asociaciones de seguridad) y renovar periódica y automáticamente la clave del cifrado simétrico entre las partes. ISAKMP generalmente utiliza IKE para crear la asociación de seguridad y negociar el algoritmo de cifrado y firma, aunque puede utilizar otros protocolos.

4.3 Técnicas y herramientas para gestión de redes

4.3.1 Consola remota, monitoreo, órdenes del servidor

El gestor de equipos e instalaciones

Un gestor de instalaciones es un conjunto de herramientas integradas entre sí y con el sistema operativo sobre el que se instala que es capaz de llevar un control exhaustivo sobre el software de cada sistema, así como de su configuración y funcionamiento.

En muchos casos, este software es capaz de controlar también los escritorios y accesos de los usuarios que se presentan en cada estación de la red. Cada fabricante de software incorpora unas funciones a sus productos de gestión; sin embargo, las funciones básicas más comunes de un gestor de equipos son las siguientes:

- Despliegue de sistemas y de software. El gestor es capaz de instalar sistemas operativos y software adicional desde los servidores de gestión en los que se apoya de acuerdo con la parametrización que diseña el administrador de sistemas.
- Configuración de los equipos. Una vez instalados los equipos, el gestor es capaz de proporcionar las configuraciones básicas de cada equipo o de cada usuario; por ejemplo, el administrador del sistema podría definir las aplicaciones a las que se tiene acceso, los recursos que serán visibles para cada usuario, etcétera.
- Control de equipos y de la red. El gestor puede analizar cada una de las incidencias ocurridas en los equipos de la red y tomar las acciones previstas por el administrador de red en cada uno de los eventos.

Con Windows Server y versiones superiores, Microsoft ha dado un gran paso adelante, integrando en su sistema herramientas avanzadas de instalación, todo ello controlado a través de una política de directivas integradas en su Directorio Activo, aunque su herramienta de gestión por excelencia para grandes redes es SMS *(Server Management System).*

Gestor de consolas remotas

Un gestor de consolas o simplemente gestor de control remoto es una aplicación que es capaz de visualizar sobre una consola local lo que está ocurriendo en una consola remota. Los más avanzados son capaces también de crear verdaderas sesiones remotas, no sólo simularlas.

Además, los gestores más avanzados son capaces de ejecutar acciones en el sistema remoto comandados desde el sistema local.

Un gestor remoto ofrece grandes ayudas; sin embargo, las funciones más beneficiadas son las siguientes:

- **Administración de red.** Desde un único punto geográfico pueden controlar todos los servidores y estaciones de la red: crear, modificar o eliminar usuarios o grupos, instalar o configurar aplicaciones, reiniciar ordenadores, etcétera.
- **Teletrabajadores.** Cualquier persona desde el exterior de la red podrá conectarse y acceder a su información de red.
- **Soporte, asistencia técnica y mantenimiento.** Estas funciones constituyen uno de los mayores ámbitos comerciales para este tipo de aplicaciones, pues se pueden brindar todos estos servicios remotamente sin necesidad de costosos desplazamientos.
- **Formación.** La tecnología utilizada por un gestor de consolas es muy apropiada para su configuración en forma de aula virtual, en el seno de la cual se pueda impartir formación. Para ello, es necesario que el gestor permita que varias sesiones locales puedan conectarse a una única sesión remota.

El transporte de red necesitado por estos gestores para mover datos a través de la red utiliza los protocolos básicos que ya hemos estudiado: TCP/IP, IPX/SPX, etc.

Destacamos la solución VNC por ser *freeware* y de amplio uso y, además, por estar soportada por muchos UNIX, Linux, Windows en todas sus variantes, OS/2, BeOS, MacOS, PalmOS y muchos más sistemas operativos.

4.3.2 Respaldo y recuperación de datos

El software más importante en las estaciones de trabajo de cualquier organización está representado por los datos de usuario, ya que cualquier aplicación puede ser reinstalada de nuevo en caso de problemas; los datos, no.

- **La duplicación de los datos.** El modo más seguro de proteger los datos ante cualquier tipo de problemas es duplicarlos. Se puede tener un doble sistema de almacenamiento en disco, pero esto genera nuevos problemas, entre los que destacamos:
  - ✓ Cuando se tiene información duplicada es difícil determinar cuál de las copias es la correcta.
  - ✓ La duplicación de información requiere la inversión de más recursos económicos, al ocupar más espacio en los dispositivos de almacenamiento.
- **Copias de seguridad.** La copia de seguridad o *backup* es una duplicación controlada de los datos o aplicaciones de los usuarios. Se realiza a través de utilidades propias de los sistemas operativos y del hardware apropiado.

  Cabe la posibilidad de que las unidades de backup estén centralizadas en los servidores, de modo que con pocas unidades se puedan realizar las copias de todo el sistema. El software de las utilidades de backup puede automatizarse para que las copias se realicen automáticamente en periodos apropiados, por ejemplo, por la noche, salvando los datos que hayan sido modificados durante el día. Los medios físicos más comunes para realizar este tipo de volcado son la cinta magnética y el CD o DVD regrabables. La relación capacidad/coste es mayor que en el caso de discos duplicados. Las desventajas residen en que la lectura de los datos de un backup no es directa por las aplicaciones y requieren un volcado inverso (de cinta a disco) previo. Se pueden establecer distintos tipos de copias de seguridad, destacamos aquí dos de ellas:
  - ✓ ***Backup* normal.** Es una copia de los archivos seleccionados sin ninguna restricción, posiblemente directorios completos y sus subdirectorios.

- ✓ ***Backup* progresivo, diferencial o incremental.** En este caso, la copia sólo se realiza sobre los ficheros seleccionados que hayan sido modificados o creados después del anterior backup.

Las copias de seguridad realizadas sobre cualquier sistema deben estar perfectamente etiquetadas y documentadas con el fin de garantizar que la recuperación de ficheros, en caso de problemas, sea de la copia correcta

La tecnología más extendida para la duplicación de discos es la RAID (*Redundant Array of Inexpensive Disks*, serie redundante de discos económicos), que ofrece una serie de niveles de seguridad o crecimiento de prestaciones catalogados de 0 a 5, aunque algunos no se utilizan:

- ✓ **RAID de nivel 0.** Los datos se reparten entre varios discos mejorando las prestaciones del acceso a disco, aunque no se ofrece ningún tipo de redundancia.
- ✓ **RAID de nivel 1.** La redundancia de datos se obtiene almacenando copias exactas cada dos discos, es decir, es el sistema de espejos al que nos hemos referido anteriormente.
- ✓ **RAID de nivel 2.** No ha sido implementado comercialmente, pero se basa en la redundancia conseguida con múltiples discos una vez que los datos se han dividido en el nivel de bit.
- ✓ **RAID de nivel 3.** Los datos se dividen en el nivel de byte. En una unidad separada se almacena la información de paridad.
- ✓ **RAID de nivel 4.** Es similar al nivel 3, pero dividiendo los datos en bloques.
- ✓ **RAID de nivel 5.** Los datos se dividen en bloques repartiéndose la información de paridad de modo rotativo entre todos los discos.

Por ejemplo, Windows NT, Windows 2000 y Windows 2003 soportan RAID 1 y RAID 5 en cualquiera de sus versiones servidoras. Microsoft denomina espejos o mirrors a RAID 1 y sistemas de bandas con paridad a RAID 5.

Para establecer discos espejo (RAID 1) sólo son necesarios dos discos, mientras que para la utilización de las bandas con paridad, el mínimo de discos es de tres.

Todas las operaciones de gestión de discos se realizan desde el administrador de discos que se halla integrado en la consola de administración local del equipo en el caso de Windows.

ACTIVIDAD

Investigue, instale, configure y presente:

Una Herramienta para visualizar y obtener métricas o estadísticas en tiempo real que le permiten visualizar, monitorizar y evaluar el funcionamiento del sistema operativo y como se da la actividad en los diferentes recursos (consumo de CPU, actividad de disco, visitas de un sitio web, tráfico, etc.) en tiempo real.

CAPÍTULO V. SOFTWARE DE APLICACIÓN

Objetivos:

- Conocer los sistemas operativos para servidores y su administración.
- Instalar y configurar un sistema operativo de manera que permita una ágil administración de recursos y usuarios.

¿De qué trata esta sesión de aprendizaje?

Con el crecimiento de la infraestructura de TIC en las organizaciones, se hace vital contar con sistemas operativos robustos que permitan administrar un gran número de usuarios y que estos a su vez puedan ejecutar todo tipo de actividades.

Estos tipos de sistemas operativos se conocen como “sistemas operativos para servidores” y se encargan de la administración de múltiples actividades en el entorno tecnológico de la organización.

5. Software de aplicación

Los sistemas operativos gestionan eficientemente los recursos del hardware, simplifican el manejo al conjunto de ordenadores y permiten una eficaz ejecución de los programas. Los administradores de sistemas son determinantes para todas las medianas y grandes empresas, ya que son los que realmente garantizan que la oficina siga con su funcionamiento diario habitual.

Como todo administrador de sistemas operativos, es crucial conocer y manejar distintos sistemas operativos, en este capítulo estudiaremos las características del sistema operativo Windows, especialmente Windows server 2016, y como este apoya las tareas del administrador de sistemas.

Windows Server 2016 añade características totalmente orientadas a la computación en la nube, aspecto fundamental en el mundo IT y de la tecnología actual. Sus áreas fundamentales son, por un lado, la mejora en la seguridad y la reducción de riesgos para el negocio, integrando varias capas de seguridad en el sistema operativo.

Por otro lado, Window Server 2016 cuenta con un centro de datos definido por un software inspirado por la tecnología de Microsoft Azure, asegurando así una reducción de costes y una mayor flexibilidad mediante la virtualización de toda la infraestructura.

Windows Server 2016. Es la última solución de Microsoft en su línea de sistemas operativos para servidores. Salió al mercado el 26 de septiembre del 2016 y su predecesor era el Windows Server 2012 R2.

Principales Novedades de Windows Server 2016

- Nanoserver. Se trata de una nueva opción que se puede utilizar a la hora de instalar el sistema operativo. Se puede administrar de forma remota y está optimizado para data centers y nubes privadas. Puede emplearse como dispositivo para máquinas con Hyper-V, servidor DNS, almacenamiento para escalabilidad, servidor web con IIS o dispositivo para aplicaciones en la nube.
- Contenedores. Es viable el manejo de contenedores de Hyper-V con un rol de Hyper-V instalado. Se pueden implementar tanto en core como en gráfica. Entre los requisitos del sistema para que funcione, necesita: 4GB de RAM, el

Server 2016, un procesador con Intel VT-X y un contenedor de los host con 2 procesadores virtuales.

- Seguridad. Permite hacer un “blindaje” de máquinas virtuales y ofrece un servicio de “guardián de dispositivos” para mayor seguridad de los datos.
- Herramientas Sysinternals. Las incluye para ayudar al administrador del servidor a resolver problemas del entorno del centro de datos. Entre las utilidades, está por ejemplo Disk2vhd, que brinda al administrador la oportunidad de convertir una imagen del sistema operativo del disco duro en un disco duro virtual.
- Habilidades de PowerShell. Las incluye gracias a un script de PowerShell FTP, el administrador puede aprovechar .NET de Windows para desplazar archivos, crear un objeto de Web Cliente y transmitir las credenciales para entrar en el servidor FTP. También permite al administrador manejar permisos de NTFS y controlar el acceso de los usuarios a una carpeta mediante el File System Security PoweShell Module.
- Storage Spaces Direct. Esta característica permite crear almacenamiento en alta disponibilidad con DAS, discos conectados directamente a cada nodo en un cluster, mediante el protocolo SMB3.
- Microsoft Passport. Este servicio reemplaza passwords con una autenticación de dos factores: Dispositivo Enrolado y una prueba Biométrica (Windows Hello) o un PIN, resultando en una mejora de seguridad en los inicios de sesión de los usuarios.
- Storage Replica. Permitirá replicar volúmenes a nivel de bloque, de forma síncrona o asíncrona.
- Windows Defender. En esta edición de Windows Server se tiene a Windows Defender presente, aunque el interfaz no viene instalado por defecto.
- Actualización mejorada para clusters de Hyper-V y almacenamiento. Permite añadir nodos Windows 2016 a un cluster 2012 R2, operando en modo Windows Server 2012 R2 hasta que todos los nodos han sido actualizados.

Mejoras

Esta nueva versión de Windows Server presume de mejoras en 3 áreas fundamentales:

- Seguridad: La mejora en la seguridad y la reducción de riesgos para el negocio se consigue integrando varias capas de seguridad en el sistema operativo.
- CPD definido por software: Inspirados por la tecnología de Microsoft Azure (Servicio en la nube de Microsoft), aseguran una reducción de costes y una mayor flexibilidad gracias a las redes, el almacenamiento y los procesos definidos por software.
- Innovación: Esta nueva versión de Windows Server incluye nuevas tecnologías como los "Contenedores" de Windows o Nano Server, que permiten nuevas formas de implementar y ejecutar aplicaciones, tanto locales como basadas en la nube.

Ediciones de Windows Server 2016

- Windows Server 2016 Standard Edition: Soporta hasta 64 sockets y hasta 4 TB de RAM, incluyendo licencias para 2 máquinas virtuales.
- Windows Server 2016 Datacenter Edition Soporta hasta 64 sockets, 640 cores y 4 TB de RAM, incluyendo licencias ilimitadas para máquinas virtuales.
- Windows Server 2016 Foundation Edition: Para pequeñas empresas, tiene un límite de hasta 15 usuarios. Soporta un número limitado de roles, un core y hasta 32 GB de RAM.
- Windows Server 2016 Essentials Edition: Se corresponde con las anteriores ediciones de Small Business Server. Esta edición puede ser instalada como un "role" en un dominio existente o como un Server en una máquina virtual. No puede funcionar como un servidor de virtualización, tampoco soporta cluster, server core o RDP server. Permite hasta 25 usuarios y 50 equipos, 2 cores y hasta 64 GB de RAM.
- Hyper-V Server 2016: Sigue siendo gratis, aunque las máquinas virtuales que se instalen deberán pagar la correspondiente licencia. Soporta hasta 64 sockets y 4 TB de RAM. Puede ser vinculado a un dominio, y como siempre

no soporta otros roles. Esta edición no tiene entorno gráfico, aunque si proporciona una limitada interfaz gráfica para una configuración básica.

- Windows Storage Server 2016 Workgroup Edition: Enfocada a ser un storage-appliance de perfil bajo. Puede ser vinculada a dominio y soporta un core, 32 GB de RAM y hasta 50 usuarios.
- Windows Storage Server 2016 Standard Edition: Soporta hasta 64 sockets, licenciada cada dos sockets. Admite hasta 4 TB de RAM e incluye dos licencias de máquinas virtuales. Puede ser vinculada a dominio y soporta algunos roles como DHCP y DNS pero puede configurarse como controlador de dominio, entidad emisora de certificados o servidor de federación.

Licencias

Windows Server 2016 viene con 3 tipos de licencias:

- Essentials: Una versión con limitaciones y pensada para organizaciones pequeñas, con menos de 25 usuarios o 50 dispositivos.
- Standard: Pensada para organizaciones que no requieren muchos servidores pero quieren un entorno robusto. Esta versión permite 2 servidores virtuales con Hyper-V e ilimitados “contenedores” de Windows.
- DataCenter: Esta es la versión por excelencia para el CPD definido por software. Permite servidores y “contenedores” ilimitados. Implementa mejoras en la virtualización: aislamiento de máquinas virtuales, mejoras en el almacenamiento definido por software y mejoras en las redes definidas por software.

5.1 Instalación de software de aplicación

Los siguientes enlaces te ayudarán a descargar e instalar diferentes versiones del sistema operativo Windows server:

- **https://www.microsoft.com/es-xl/evalcenter/evaluate-windows-server-2016**

ACTIVIDAD

Tema: Instalación y configuración del S.O

El grupo de alumnos deberá realizar la instalación y configuración de una Plataforma Operativa Linux, o Windows en Distribución y Versión a elección del grupo de trabajo. Se recomienda el uso de Windows Server 2016, o cualquiera que se justifique su instalación.

La asignación constará de dos etapas, la instalación y otra posterior de respuesta a los ejercicios propuestos.

La instalación puede hacerse:

- Instalación real en HDD privados, determinados por el grupo.
- Instalación a través de Virtualización. (Recomendada).
- No hay una configuración pre-establecida de Hardware, la elección es libre.

Debe completar y responder los siguientes puntos:

- Ventajas y Desventajas del sistema instalado.
- Datos de la configuración de Hardware seleccionada para la instalación.
- Listado impreso de la configuración de Hardware y software.
- Creación de 2 usuarios, los cuales deben tener capacidad de administración.
- Creación de 2 grupos y asignarles permisos o privilegios sobre carpetas.
- Crear y compartir 2 carpetas.

CAPÍTULO VI. ADMINISTRACIÓN DE ARCHIVOS Y RESPALDOS

Objetivos:

- Apreciar la importancia de la gestión eficiente de archivos y su impacto en el rendimiento del sistema.
- Explorar los métodos o técnicas que ayudan al administrador de sistemas operativos a gestionar los archivos y respaldos y de esta manera mejorar el rendimiento del sistema.

¿De qué trata esta sesión de aprendizaje?

Los archivos tienen vida fuera de cualquier aplicación individual que los utilice para entrada y salida. Los usuarios desean poder acceder a los archivos, guardarlos y mantener la integridad de su contenido. Como ayuda a estos objetivos, virtualmente todos los sistemas de computadores proporcionan sistemas específicos de gestión de ficheros. Normalmente, cada sistema dispone de programas de utilidad que se ejecutan como aplicaciones privilegiadas. Sin embargo un sistema de gestión de archivos necesita como mínimo algunos servicios especiales del sistema operativo. En este capítulo se abordará la gestión de archivos, las funciones, características y beneficios que le ofrece esta al rendimiento del sistema.

6. Administración de archivos y respaldos

6. Introducción

La tecnología no está exenta de fallas o errores, y los respaldos de información son utilizados como un plan de contingencia en caso de que una falla o error se presente.

Asimismo, hay empresas, que por la naturaleza del sector en el que operan (por ejemplo Banca) no pueden permitirse la más mínima interrupción informática.

Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones, etc. Y aunque no se pueda prevenir cada una de estas interrupciones, la empresa sí puede prepararse para evitar las consecuencias que éstas puedan tener sobre su negocio. Del tiempo que tarde en reaccionar una empresa dependerá la gravedad de sus consecuencias.

Además, podríamos recordar una de las leyes de mayor validez en la informática, la "Ley de Murphy":

- Si un archivo puede borrarse, se borrará.
- Si dos archivos pueden borrarse, se borrará el más importante.
- Si tenemos una copia de seguridad, no estará lo suficientemente actualizada.

La única solución es tener copias de seguridad, actualizarlas con frecuencia y esperar que no deban usarse.

Respaldar la información significa copiar el contenido lógico de nuestro sistema informático a un medio que cumpla con una serie de exigencias:

- Ser confiable: Minimizar las probabilidades de error. Muchos medios magnéticos como las cintas de respaldo, UBS, o discos duros tienen probabilidades de error o son particularmente sensibles a campos magnéticos, elementos todos que atentan contra la información que hemos respaldado allí. Otras veces la falta de confiabilidad se genera al rehusar los medios magnéticos. Las cintas en particular tienen una vida útil concreta. Es común que se subestime este factor y se reutilicen más allá de su vida útil, con resultados nefastos, particularmente porque vamos a descubrir su falta

de confiabilidad en el peor momento: cuando necesitamos RECUPERAR la información.

- Estar fuera de línea, en un lugar seguro: Tan pronto se realiza el respaldo de información, el soporte que almacena este respaldo debe ser desconectado de la computadora y almacenado en un lugar seguro tanto desde el punto de vista de sus requerimientos técnicos como humedad, temperatura, campos magnéticos, como de su seguridad física y lógica. No es de gran utilidad respaldar la información y dejar el respaldo conectado a la computadora donde potencialmente puede haber un ataque de cualquier índole que lo afecte.
- La forma de recuperación sea rápida y eficiente*:* Es necesario probar la confiabilidad del sistema de respaldo no sólo para respaldar sino que también para recuperar. Hay sistemas de respaldo que aparentemente no tienen ninguna falla al generar el respaldo de la información pero que fallan completamente al recuperar estos datos al sistema informático. Esto depende de la efectividad y calidad del sistema que realiza el respaldo y la recuperación.

Esto nos lleva a que un sistema de respaldo y recuperación de información tiene que ser probado y eficiente.

Por otro lado, la administración de archivos, es el componente del sistema operativo encargado de administrar y facilitar el uso de las memorias periféricas, ya sean secundarias o terciarias. Sus principales funciones son la asignación de espacio a los archivos, la administración del espacio libre y del acceso a los datos resguardados.

Estructuran la información guardada en una unidad de almacenamiento (normalmente un disco duro de una computadora), que luego será representada ya sea textual o gráficamente utilizando un gestor de archivos. La mayoría de los sistemas operativos manejan su propio sistema de archivos.

El sistema de archivos se basa en la administración de clústers, la unidad de disco más chica que el sistema operativo puede administrar. Un clúster consiste en uno o más sectores. Por esta razón, cuanto más grande sea el tamaño del clúster,

menores utilidades tendrá que administrar el sistema operativo. Por el otro lado, ya que un sistema operativo sólo sabe administrar unidades enteras de asignación (es decir que un archivo ocupa un número entero de clústers), cuantos más sectores haya por clúster, más espacio desperdiciado habrá. Por esta razón, la elección de un sistema de archivos es importante. La estructura de directorios suele ser jerárquica, ramificada o “en árbol”, aunque en algún caso podría ser plana.

En algunos sistemas de archivos los nombres de archivos son estructurados, con sintaxis especiales para extensiones de archivos y números de versión. En otros, los nombres de archivos son simplemente cadenas de texto y los metadatos de cada archivo son alojados separadamente.

6.1 Archivos

Los archivos o ficheros son unas unidades lógicas de almacenamiento que define el propio sistema operativo. Se estructuran como una serie de bits, cuyo significado está definido por su creador. Un sistema de gestión de archivos facilita a los usuarios y aplicaciones, servicios para el uso y control de accesos a directorios y archivos.

El sistema operativo proporciona una vista lógica uniforme del almacenamiento de la información, haciendo una abstracción de las propiedades físicas de los dispositivos de almacenamiento para definir una unidad de almacenamiento lógica. El sistema operativo hace un mapa de los archivos en los medios físicos y accede a estos archivos a través de los dispositivos de almacenamiento.

Los archivos se pueden estructurar de varias maneras las más comunes son,

- Secuencia de bytes. El archivo es una serie no estructurada de bytes. Posee máxima flexibilidad. El sistema operativo no sabe que contiene el archivo.
- Secuencia de registros. El archivo es una secuencia de registros de longitud fija, cada uno con su propia estructura interna.
- Árbol. El archivo consta de un árbol de registros, no necesariamente de la misma longitud. Cada registro tiene un campo llamado key (llave o clave) en una posición fija del registro. El árbol se ordena mediante el campo clave para permitir una rápida búsqueda de una clave particular.

6.2 Sistemas de gestión de archivos

Con la tan demandada incorporación de las TIC a los procesos de producción y gestión, muchas empresas e instituciones han modificado sustancialmente los modos y maneras de trabajo. Este hecho tiene diversas e importantes repercusiones en los actuales servicios de información y documentación y en los profesionales encargados de gestionar el conocimiento.

Se considera que la información interna y externa, es un elemento estratégico dentro de las organizaciones que aporta competitividad para las mismas. Las diversas formas de los documentos electrónicos, tipologías y adecuación de las actuales herramientas informáticas para la gestión integral de la documentación circulante, son factores esenciales para analizar detenidamente por parte de los servicios de información y documentación de toda institución a la hora del diseño de un sistema de gestión electrónica de archivos; estas ideas cobran una especial importancia en nuestros días.

El valor actual del documento dentro de las organizaciones viene derivado de las características que determinan a los actuales documentos electrónicos, entre las que se destacan:

- Combinación de diferentes unidades de información (texto, sonido, imágenes y videos)
- Legibles por máquinas y no por personas
- Puede cambiar de soporte con el tiempo
- Establece relaciones con otros documentos
- Puede ser modificado y reproducido con facilidad
- Admite múltiples formatos de lectura, estructurales y estéticos

Actualmente se habla de documentos inteligentes como contenedores dinámicos de conjuntos de información, creados por distintas aplicaciones que se revisan y actualizan de manera automática. En este entorno conceptual aparecen en el mercado, distintos productos informáticos orientados al control y la gestión integral de la documentación, conocidos por sistemas o herramientas de GED (Gestión

Electrónica de Documentos) o por el término anglosajón de EDMS (Electronic Document Management Systems).

Objetivos

Un sistema de gestión de archivos debe considerar los siguientes objetivos generales para cubrir las necesidades básicas de una organización:

- Facilitar el trabajo a los usuarios con los documentos, permitiéndoles de manera sencilla guardar y encontrar en poco tiempo los documentos cuando los necesiten.
- Promover que la información se comparta y se aproveche como un recurso colectivo, evitando que se duplique.
- Conservar la memoria de la organización más allá de los individuos aprovechando la experiencia acumulada.

Funciones

Un sistema de gestión de archivos, para que sea eficaz y llegue a un mejoramiento de resultados en la organización debe considerar los siguientes aspectos:

- Determinar si un documento, creado o recibido por la organización, debe conservarse.
- Dejar constancia de la incorporación de un documento en el sistema mediante un identificador único y datos esenciales que permitan su posterior ubicación.
- Identificar la categoría a la que pertenece un documento teniendo en cuenta la actividad de la organización con la que está relacionado y de la cual es evidencia.
- Almacenar los documentos en función de su soporte y formato, su uso y su valor, de manera que se asegure su autenticidad, fiabilidad, integridad y disponibilidad durante el periodo de tiempo necesario.
- Determinar a quién está permitido el acceso a los documentos y en qué circunstancias, mediante controles apropiados.
- Controlar el uso y movimiento de los documentos de manera que se garantice que los usuarios con permisos adecuados realizan tareas para las que han sido autorizados.

- Determinar la conservación de los documentos, así como también los procedimientos a seguir para: destrucción física, traslado a otro sistema de almacenamiento, transferencia a otra unidad u organización.

Características

La norma ISO 15489-1, publicada en el 2001, bajo el título "Information and Documentation: Records Management: Part 1", proporciona una guía sobre cómo gestionar o administrar los documentos y su relación con los sistemas electrónicos para la conservación de archivos en diferentes soportes.

El objetivo de esta norma es establecer las políticas, procedimientos y prácticas de la administración de documentos de archivo con el fin de asegurar su adecuada atención y protección, y permitir que la evidencia y la información que contienen puedan recuperarse de un modo más eficiente y eficaz.

Dentro de las características que sugiere la norma se tiene las siguientes:

- Fiabilidad: Cualquier sistema de administración de documentos de archivo, debe funcionar de modo regular y continuado mediante procedimientos fiables.
- Integridad: Deben aplicarse medidas para controlar la disponibilidad de la información, la identificación del usuario, la destrucción autorizada y la seguridad, con la finalidad de evitar el acceso, la destrucción, la modificación o la eliminación no autorizada.
- Conformidad: Debe cumplir todos los requisitos derivados de las actividades propias de una organización, de su entorno normativo y de las expectativas de la sociedad. El personal que elabora documentos de archivo, debe saber cómo afectan estos requisitos a las acciones que se realizan.
- Exhaustividad: Debe gestionar los documentos procedentes de todas las actividades de una organización o de una sección que forma parte de ella.
- Carácter sistemático: Los documentos de archivo se deben crear, conservar y gestionar sistemáticamente, para lo cual es necesario establecer una asignación de responsabilidades y metodologías formalizadas para su gestión.

Beneficios

La implementación de un sistema de gestión de archivos provee a corto y largo plazo un cúmulo de beneficios como:

- Elimina la pérdida de documentos.
- Varios usuarios pueden consultar el mismo documento simultáneamente.
- Acelera el acceso a cualquier documento.
- Manejo de índices de búsqueda de la información.
- Resguardar sus documentos en diversos formatos electrónicos.
- Controlar el acceso a la información por niveles de seguridad.
- Eliminación de los documentos duplicados.

6. 3 Organización y acceso archivos

Desde la perspectiva de un usuario, un archivo es la porción más pequeña de almacenamiento secundario lógico, es decir, no pueden escribirse datos en almacenamiento secundario a menos que se encuentre dentro de un archivo .La información de un archivo es definida por su creador. En un archivo se pueden almacenar diferentes tipos de información: programas fuente, programas objeto, programas ejecutables, datos numéricos, texto, registros e nomina, imágenes, grabaciones de sonido, etc.,

Un archivo recibe un nombre, para conveniencia de sus usuarios, y se hace referencia a el por dicho nombre. Un nombre es generalmente una cadena de caracteres. Algunos sistemas distinguen entre mayúsculas y minúsculas en los nombres, en tanto que otros sistemas consideran los dos casos como equivalentes. Cuando se asigna un nombre a un archivo, este se vuelve independiente del proceso del usuario, e incluso del sistema que lo creo.

Un archivo tiene generalmente los siguientes atributos:

- Nombre. El nombre simbólico del archivo es la única información que se mantiene en forma legible para los humanos.
- Tipo. Esta información es necesaria para aquellos sistemas que soportan diferentes tipos.

- Ubicación. Esta información es un apuntador a un dispositivo y a la ubicación del archivo en dicho dispositivo.
- Tamaño. En este atributo se incluyen el tamaño actual del archivo (en bytes, palabras o bloques) y, posiblemente, el tamaño máximo permitido.
- Protección. Información de control de acceso que determina quién puede leer, escribir, ejecutar, etc. El archivo.
- Hora, fecha e identificación del usuario. Esta información puede mantenerse para La creación, la última modificación, el último uso.

Estos datos pueden ser útiles para protección, seguridad y control de uso.

Para definir adecuadamente a los archivos, necesitamos considerar las operaciones que se pueden realizar sobre ellos.

El sistema operativo proporciona llamadas al sistema para crear, escribir, leer, reposicionar, borrar y truncar archivos"

Operaciones básicas sobre archivos:

- Crear un archivo: Se debe encontrar espacio para el archivo en el sistema de archivos y posteriormente se debe hacer una entrada en el directorio para el nuevo archivo. La entrada en el directorio registra el nombre del archivo y su ubicación en el sistema de archivos.
- Escribir u archivo: Se hace una llamada al sistema especificando tanto el nombre del archivo como la información que se va a escribir en el. El sistema debe mantener un apuntador de escritura a la ubicación en el archivo donde va a tener un lugar la siguiente escritura. El apuntador de escritura debe actualizarse siempre que ocurra una escritura.
- Leer un archivo: Se hace una llamada al sistema que especifica el nombre del archivo y el lugar (en la memoria) donde deberá colocarse el siguiente bloque del mismo. Nuevamente, se busca en el directorio la entrada asociada y el sistema mantiene un apuntador de lectura a la ubicación en el archivo en donde va a tener lugar la siguiente lectura. Una vez que se ha realizado la operación, el apuntador de lectura se actualiza. Tanto la operación de lectura como la de escritura emplean este mismo apuntador, ahorrando espacio y reduciendo la complejidad del sistema.

- Reposicionarse dentro de un archivo. Se busca en el directorio la entrada apropiada y se asigna un valor dado a la posición actual del archivo. El reposicionamiento dentro de un archivo no necesita incluir una operación real de E/S. Está operación sobre el archivo también se conoce como búsqueda en archivo.
- Borrar un archivo. Se busca en el directorio el archivo designado. Una vez que se ha encontrado la entrada asociada, se librera todo el espacio del archivo (para que pueda ser utilizado por otros archivos) y se borra la entrada del directorio.
- Truncar un archivo. Hay ocasiones en que el usuario desea que los atributos de un archivo permanezcan iguales, pero quiere borrar el contenido del archivo. En lugar de obligar al usuario a borrar el archivo y después volver a crearlo, esta función permite que todos los atributos permanezcan sin modificación (excepto la longitud del archivo), pero restableciendo el archivo a longitud cero.

Las funciones principales de la Organización del Archivo:

- Reducir la duplicidad de los documentos,
- Localizar de forma rápida oportuna documentos importantes
- Optimizar los espacios conservando únicamente los documentos realmente importantes, y sólo por el plazo que deban ser conservados.

A continuación una descripción resumida de cada uno de sus componentes de la organización de un archivo.

- Fondo: Es el lugar donde se encuentra la totalidad de la documentación producida por una institución o persona. Cada fondo precisará de un cuadro de clasificación, una ordenación de sus series, y de una descripción completa (guía e inventario).
- Sección: Es el conjunto de documentos generados en razón de la actividad de una subdivisión orgánica o funcional. La sección es una parte del fondo que tiene su sitio en el inventario.

- Serie: Es el testimonio documental de las actividades realizadas por un organismo según su función. Cada sección se encuentra conformada por documentos agrupados en series.
- Expediente: Es el conjunto ordenado de documentos condicionados a un proceso administrativo iniciado por un usuario para la solución de un mismo asunto o trámite de interés común del organismo de destino. Los expedientes deben ser ordenados de forma alfabética por nombres de personas u organismos por ejemplo: expedientes académicos de alumnos. Los expedientes ya tramitados por toda la unidad deben almacenarse en cajas tipo archivo definitivo, en cuyo lomo se anotará el organismo productor, título de la serie, años, expedientes que contienen y el número de orden de las cajas.
- Documentos: Desde el punto de vista de una organización, un documento es el elemento esencial para su funcionalidad, ya que la información que contienen es vital para su operación diaria, a continuación se muestra una posible organización del Archivo.

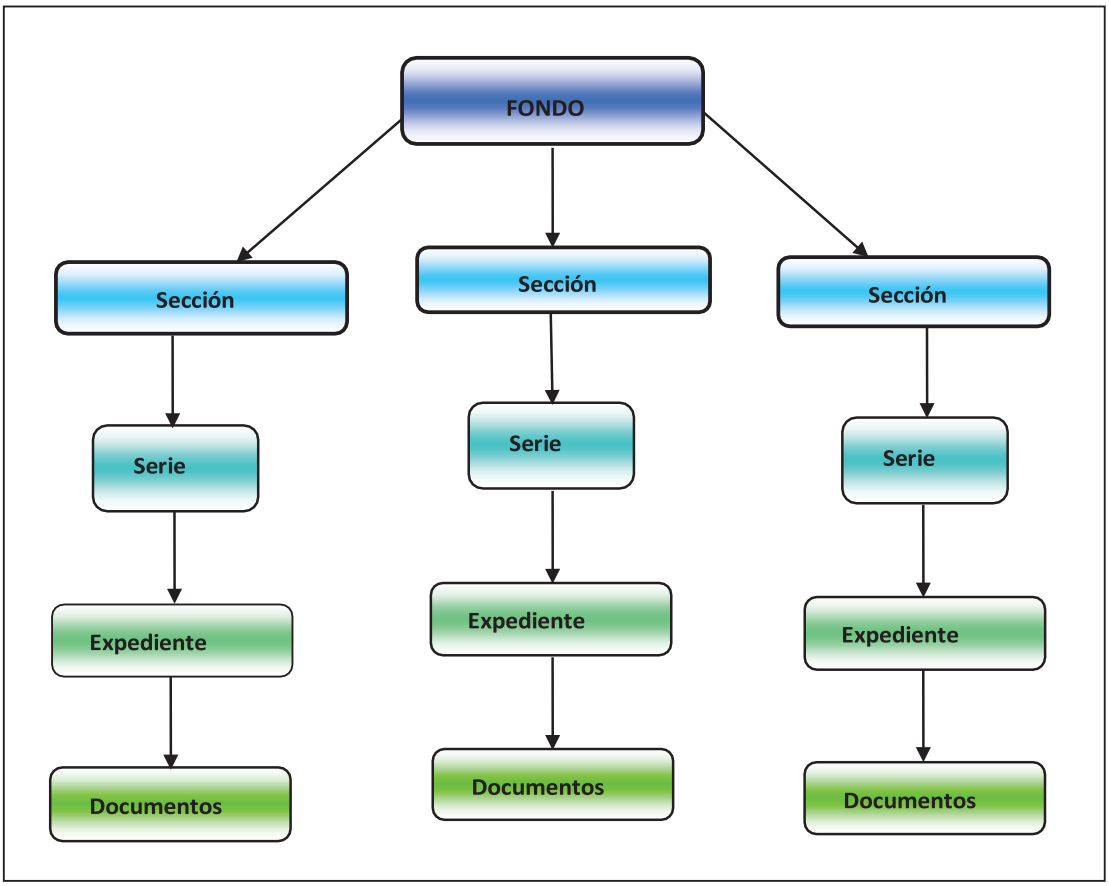

Figura 3. Organización del Archivo

6.4 Administración de archivos en ambientes de clusters y nubes.

Se define la administración de archivos como el conjunto de procesos a realizar para administrar documentos y archivos dentro de una organización apoyados en un conjunto de normas técnicas y prácticas.

En este sentido, la implementación correcta de la gestión documental permite recuperar cómodamente la información contenida en los documentos, modificarla si es necesario y archivarla el tiempo que sea necesario. De este modo, usando criterios básicos de economía y racionalización, es más sencillo determinar cuáles se pueden eliminar para ahorrar espacio ya que, en un momento dado, dejan de tener utilidad, y cuáles deben quedar guardados por su mayor valía.

Este es el concepto de gestión documental, pero lógicamente en la actualidad, cuando lo relacionamos con Internet y las plataformas de almacenamiento online

que existen, entendemos por gestión documental algo más amplio en cuanto a su utilidad y rentabilidad para empresas, instituciones y administraciones, es lo que podríamos definir como gestión documental en la nube.

Consideraciones al implantar un Sistema de administración de archivos basado en la nube en su organización

Pasar del papel o las carpetas compartidas en un servidor a un Sistema de Gestión Documental es a menudo un proyecto largo. Aquí van algunos pasos recomendados:

- Planificación del Sistema de Gestión Documental.
- Clasificación de los documentos de la organización por categorías.
- Análisis de cada categoría
    - ✓ Qué nombre y código queremos darle a los documentos de ese tipo
    - ✓ Qué proceso siguen esos documentos (diagrama de estados)
    - ✓ Qué agentes: personas internas (usuarios) y externas (clientes, proveedores…) están involucradas en los diferentes pasos del proceso.
    - ✓ Qué metadatos (campos de datos) deben rellenarse o extraerse de cada documento de esa categoría para poder buscar y localizar con rapidez, generar plantillas o extraer informes.
    - ✓ Qué plantillas o modelos se utilizan y pueden automatizarse
    - ✓ Qué comunicaciones pueden automatizarse entre los agentes del proceso (correos electrónicos automáticos)
    - ✓ Qué técnicas de gestión documental merece la pena utilizar para esta categoría de documentos (Firma digital, control de versiones)
    - ✓ Permisos y seguridad para este tipo de documento en las carpetas correspondientes.

- Durante el trabajo
    - ✓ Creación de nuevos documentos, generación automática de plantillas, digitalización o escaneo de originales.

- ✓ Identificación visual del estado de los documentos en su proceso(códigos y colores)
- ✓ Cambios de estado en los documentos: manuales y automáticos (avance por el proceso)
- ✓ Búsquedas y consultas por metadatos, categorías, carpetas, etc.
- ✓ Exportación de metadatos a herramientas de ofimática (tablas Excel)

- Control, mejora y resolución de problemas
  - ✓ Rendimiento y mejora del proceso (localizar cuellos de botella, estados o campos que faltan o sobran en cada proceso)
  - ✓ Trazabilidad del proceso (quién, cuándo, cómo hizo cualquier acción o cambio de estado)

Toma de Decisiones en la Nube

- Recolectar datos sobre los servicios de cómputo en la nube y modelos de despliegue, así como de los proveedores de servicios en la nube.
- Llevar a cabo una evaluación de la organización para identificar cuáles documentos de archivo, aplicaciones y procesos son potenciales candidatos para migración al entorno de nube;
- Determinar cuáles servicios en la nube y modelos de despliegue son aptos para el modelo de negocio de su organización, su gobernanza y los requisitos de cumplimiento;
- Llevar a cabo una evaluación de riesgos para los documentos de archivo, aplicaciones y procesos en caso de trasladarse a la nube, incluyendo la identificación, análisis y desarrollo de un plan de respuesta al riesgo;
- Llevar a cabo un proyecto piloto en la nube para la organización, moviendo los registros identificados, aplicaciones y procesos hacia el entorno de nube;
- Tomar en cuenta la serie de cuestiones que deben preverse para la continua administración de archivos, aplicaciones y procesos ya trasladados a la nube, incluyendo la gestión documental y la clasificación, el cumplimiento, el seguimiento y la auditoría, la seguridad y el acceso permanente;

- Antes de mover los documentos de archivo, aplicaciones o procesos a la nube, las organizaciones deben garantizar que los procedimientos son adecuados para obtener información de los sistemas del proveedor de nube y ser transferidos a otro proveedor de servicios o hacia la organización.

Caso de Uso

Una organización de tipo industrial enfrentó en un momento dado el tratamiento de un número excesivo de archivos. Más de 4.000 documentos relacionados con sus procedimientos y procesos, debían ser gestionados.

Sin embargo, se cometieron muchos errores derivados de la acumulación de documentación obsoleta e innecesaria, la falta de control, inconsistencias en los registros antiguos y la falta de entrenamiento de los empleados encargados de la labor.

Cuando esta organización optó por implementar un sistema de gestión de archivos, la organización no solo pudo mantener sus documentos a salvo y en una ubicación accesible desde cualquier lugar y en cualquier momento, sino que también fue capaz de mejorar el índice de rendimiento y desempeño. En cuanto a la calidad exactamente, la organización obtuvo los siguientes resultados:

Aumento del 25 % en eficiencia.

Reducción hasta de un 10 % de los defectos, gracias a la actualización de muchos documentos.

Antes de que esta organización implementará un sistema de gestión de archivos, ¿cómo califica usted el rendimiento de la administración de sistemas? Justifique su respuesta.

¿Cree usted que es necesario utilizar un sistema de gestión de archivos en los Sistemas de información actuales? Justifique su respuesta.

ACTIVIDAD

Investigue y presente una aplicación o sistema que permita el respaldo en la nube y presente los siguientes criterios utilizados en el control de documentos en los Sistemas de Gestión.

Debe presentar la configuración de los siguientes criterios:

- Agrupación por proyecto, cliente, producto y fecha.
- Indexación. ¿Cómo buscar?
- Limitación de acceso. ¿Quién puede ver y cuándo?
- Almacenamiento y mantenimiento en la nube
- Periodos de almacenamiento de documentos antiguos.
- Inutilización y disposición del archivo antiguo.
- Controles para la seguridad.
- Personalización de la plataforma

CAPÍTULO VII. ARCHIVOS Y RESPALDOS

Objetivos:

- Analizar los riesgos a los que comúnmente se encuentran amenazados los sistemas de información.
- Clasificar los tipos de respaldos que puede poner en marcha el administrador de sistema para mantener la disponibilidad de la información.
- Enumerar los dispositivos y tecnologías de almacenamiento que se encuentran disponibles para realizar esta labor.

¿De qué trata esta sesión de aprendizaje?

Uno los aspectos que es necesario considerar en la administración de sistemas operativos, es la forma en la cual se almacenarán y respaldarán los datos que serán generados o recopilados.

Al hacer esto, es importante tener en cuenta que los medios de almacenamiento y respaldo podrán variar dependiendo a las necesidades de los sistemas, a la organización y sus recursos.

Los medios de almacenamiento y respaldo que se pueden utilizar no son excluyentes, por lo que pueden complementarse entre sí.

7. Archivos y respaldos

7.1 Riesgo en los cuales se encuentran inmersos los Sistemas de Información

El riesgo es la probabilidad que un peligro (causa inminente de pérdida), existente en una actividad determinada durante un período definido, ocasione un incidente de ocurrencia incierta pero con consecuencias factibles de ser estimadas.

También lo podemos entender, como el potencial de pérdidas que existe asociado a una operación productiva, cuando cambian en forma no planeada las condiciones definidas como estándares para garantizar el funcionamiento de un proceso o del sistema productivo en su conjunto.

Por todo lo anterior para las organizaciones es imprescindible identificar aquellos riesgos relevantes a los cuales se pueda ver enfrentado y que conlleven un peligro para la consecución de sus objetivos, más aún cuando la rentabilidad de su negocio está íntimamente ligada a dichos riesgos.

- **Riesgos de Integridad:**

  Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización.

- **Riesgos de Relación:**

  Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de base de datos y los riesgos asociados a la confidencialidad de la información.

- **Riesgos de acceso:**

  Estos se relacionan directamente a la información de toma de decisiones (información y datos correctos de una persona y sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

- **Riesgo de utilidad:**

  Estos riesgos se enfocan entres diferentes niveles de riesgos: los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que

los problemas ocurran. Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas. Backups y planes de contingencia controlan desastres en el procesamiento de la información.

- **Riesgos de infraestructura:**

  Estos riesgos se refieren a que en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente.

7.2 Clasificación de respaldos

Los respaldos o copias de seguridad tienen dos objetivos principales:

- Permitir la restauración de archivos individuales
- Permitir la restauración completa de sistemas de archivos completos

El primer propósito es la base para las peticiones típicas de restauraciones de archivos: un usuario accidentalmente borra un archivo y le pide restaurarlo desde el último respaldo. Las circunstancias exactas pueden variar, pero este es el uso diario más común de los respaldos.

La segunda situación es la peor pesadilla de un administrador de sistemas: por la situación que sea, el administrador se queda observando un hardware que solía ser una parte productiva del centro de datos. Ahora, no es más que un pedazo de acero y silicon inútil. Lo que está faltando en todo el software y los datos que usted y sus usuarios habían reunido por años. Supuestamente todo ha sido respaldado. La pregunta es: ¿Está seguro? Y si lo ha sido, ¿Lo puede restaurar?

Datos diferentes: Necesidades de respaldos diferentes

Observe el tipo de datos procesados y almacenados por un sistema computacional típico. Observe que algunos de los datos raramente cambian y otros cambian constantemente.

El ritmo al cual los datos cambian es crucial para el diseño de un procedimiento de respaldo. Hay dos razones para esto:

- Un respaldo no es más que una instantánea de los datos respaldados. Es un reflejo de los datos en un momento particular.

- Los datos que cambian con poca frecuencia se pueden respaldar menos a menudo, mientras que los datos que cambian regularmente deben ser copiados frecuentemente.

Los administradores de sistemas que tienen un buen entendimiento de sus sistemas, usuarios y aplicaciones deberían ser capaces de agrupar rápidamente en sus sistemas en diferentes categorías. Sin embargo, he aquí algunos ejemplos para comenzar:

Si le pregunta a una persona que no está familiarizada con los respaldos o copias de seguridad de computadoras, la mayoría pensaría que un respaldo es una copia idéntica de *todos* los datos en un computador. En otras palabras, si se creó un respaldo el martes en la noche, y no se cambió nada durante el miércoles completo, el respaldo del miércoles en la noche sería idéntico que el del martes.

Mientras que es posible configurar los respaldos de esta forma, es probable que no lo haga. Para entender un poco más sobre esto, primero se debe entender los **tipos de respaldo** que se pueden crear. Estos son:

- Respaldos completos
- Respaldos incrementales
- Respaldos diferenciales

Respaldos completos

El tipo de respaldo discutido al principio de esta sección se conoce como *respaldo completo*. Un respaldo completo es un respaldo donde cada archivo es escrito a la media de respaldo. Como se mencionó anteriormente, si los datos a respaldar nunca cambian, cada respaldo completo creado será una copia de exactamente lo mismo.

Esta similaridad se debe al hecho de que un respaldo completo no verifica para ver si un archivo ha cambiado desde el último respaldo; ciegamente escribe todo a la media de respaldo, haya sido modificada o no.

Esta es la razón por la que los respaldos completos no se hacen todo el tiempo cada archivo es escrito a la media de respaldo. Esto significa el uso de gran cantidad de media de respaldo aun cuando nada se haya cambiado. Respaldar 100 GB de datos

cada noche cuando solamente cambió 10 MB de datos, no es una buena solución; por eso es que se crean los *respaldos incrementales*.

Respaldos incrementales

A diferencia de los respaldos completos, los respaldos incrementales primero revisan para ver si la fecha de modificación de un archivo es más reciente que la fecha de su último respaldo. Si no lo es, significa que el archivo no ha sido modificado desde su último respaldo y por tanto se puede saltar esta vez. Por otro lado, si la fecha de modificación *es* más reciente, el archivo ha sido modificado y se debería copiar.

Los respaldos incrementales son utilizados en conjunto con respaldos regulares completos (por ejemplo, un respaldo semanal completo, con respaldos incrementales diarios).

La principal ventaja obtenida de los respaldos incrementales es que se ejecutan muchísimo más rápido que un respaldo completo. La principal desventaja es que restaurar un archivo dado puede implicar pasar a través de varios respaldos incrementales hasta encontrar el archivo. Cuando se restaura un sistema de archivos completo, es necesario restaurar el último respaldo completo y cada respaldo incremental subsecuente.

En un intento de aliviar la necesidad de pasar a través de varios respaldos incrementales, se puede utilizar un enfoque ligeramente diferente. Esto se conoce como *respaldo diferencial*.

Respaldos diferenciales

Los respaldos diferenciales son similares a los respaldos incrementales en que ambos solamente copian archivos que han sido modificados. Sin embargo, los respaldos diferenciales son *acumulativos,* en otras palabras, con un respaldo diferencial, una vez que un archivo ha sido modificado continua siendo incluido en todos los respaldos diferenciales subsecuentes (hasta el próximo respaldo completo).

Esto significa que cada respaldo diferencial contiene todos los archivos modificados desde el último respaldo completo, haciendo posible realizar una restauración completa solamente con el último respaldo completo y el último respaldo diferencial.

De la misma manera que la estrategia de respaldo de los respaldos incrementales, los respaldos diferenciales siguen el mismo enfoque: un respaldo completo periódico seguido de más frecuentes respaldos diferenciales.

El efecto de utilizar los respaldos diferenciales de esta forma es que los respaldos diferenciales tienden a crecer un poco con el tiempo (asumiendo que diferentes archivos son modificados con el paso del tiempo entre respaldos completos). Esto coloca los respaldos diferenciales en un punto entre los respaldos incrementales y los completos en términos de utilización de la media y velocidad de los respaldos, mientras que ofrecen restauraciones completas y de archivos individuales mucho más rápidas (debido a que hay menos respaldos en los que buscar/restaurar).

Dadas estas características, vale la pena considerar cuidadosamente los respaldos diferenciales.

7.3 Dispositivos de almacenamiento

Tecnologías: óptica y magnética u otras de almacenamiento

Cintas

Las cintas fueron el primer tipo de media removible disponible como medio de almacenamiento. Tiene los beneficios de bajos costos y una capacidad de almacenamiento razonablemente buena. Sin embargo, las cintas tienen algunas desventajas, es susceptible a desgastarse y el acceso a los datos en una cinta es por naturaleza secuencial.

Estos factores implican que es necesario hacer un seguimiento del uso de las cintas (retirando las cintas una vez que hayan alcanzado el final de su vida útil) y que las búsquedas de un archivo en cinta pueden ser una tarea bastante lenta.

Por otro lado, las cintas son uno de los medios de almacenamiento masivo menos costosos disponibles y tienen una larga historia de confiabilidad. Esto significa que construir una biblioteca de cintas de un buen tamaño no necesita consumir una gran parte de su presupuesto, y puede contar con poderla utilizar ahora y en un futuro.

Disco

En años pasados, las unidades de disco nunca se utilizaban como medio para respaldos. Sin embargo, los precios se han reducido tanto que, en algunos casos, el uso de discos duros como unidades de respaldo, tiene sentido.

La razón principal para el uso de unidades de disco como medio para respaldos sería su velocidad. No hay un medio de almacenamiento masivo más rápido disponible. La velocidad puede ser un factor crítico cuando la ventana para hacer el respaldo de su centro de datos es corta y la cantidad de datos a copiar es grande.

Pero por varias razones el almacenamiento en disco no es el medio ideal para respaldos.

- Normalmente los discos duros no son removibles. Un factor clave para una estrategia de respaldo efectiva es que se pueda retirar la media de su centro de datos y en algún tipo de almacenamiento fuera del sitio. Un respaldo de la base de datos de producción sentada en un disco duro medio metro más allá de la base de datos misma no es un respaldo; es una copia. Y las copias no son muy útiles si los datos del centro de datos y sus contenidos (incluyendo las copias) son dañadas o destruidas por algún tipo de evento desafortunado.
- Las unidades de disco duro son costosas (al menos comparados con otros tipos de medios). Hay situaciones donde el dinero realmente no es un problema, pero en todos los demás casos, los costos asociados con el uso de discos duros para respaldos significa que el número de copias de respaldo se debe mantener bajo para así mantener bajos los costos generales. Menos copias de seguridad significa menos redundancia si por alguna razón uno de los respaldos no se puede leer.
- Los discos duros son frágiles. Aún si hace el gasto adicional de comprar discos removibles, su fragilidad puede ser un problema. Si se le cae un disco, usted perdió el respaldo. Es posible comprar estuches especiales que pueden reducir (pero no eliminar completamente) este peligro, pero esto hace una propuesta costosa aún más costosa.
- Las unidades de disco no son media para archivado. Asumiendo que pueda superar todos los otros problemas asociados con la realización de respaldos

a unidades de disco, debería considerar lo siguiente. La mayoría de las organizaciones tienen varios requerimientos legales para mantener los registros disponibles por cierto tiempo. Las posibilidades de obtener data utilizable desde una cinta de 20 años son mucho más grandes que las posibilidades de hacerlo desde un disco de 20 años. Por ejemplo, ¿tendrá el hardware necesario para conectarlo a su sistema? Otra cosa a considerar es que una unidad de disco es mucho más compleja que una unidad de cinta. Cuando un motor de 20 años gira un plato de disco de 20 años, causando que los cabezales de lectura/escritura de 20 años vuelen sobre la superficie del plato, ¿cuáles son las posibilidades de que estos componentes funcionen sin problema después de haber estado 20 años sentados sin hacer nada?

Discos duros / SSD USB

La unidad USB es de confianza y uno de los favoritos por buenas razones.

Son rápidos (si usted va para un modelo de 3.0 USB), que soportan todos los tipos de trabajo y te permitirán crear una estrategia de copia de seguridad simple, fiable fuera del sitio sin que realmente cueste.

Otra razón es que si necesita tener acceso a una copia de seguridad, puede simplemente conectar a cualquier ordenador con Windows y no hay ningún hardware especializado necesario para restaurar los datos.

Por último, pero no menos importante, si usted decide ir por la vía USB, no olvide llevar siempre un repuesto.

Unidades RDX

RDX se está convirtiendo en una opción cada vez más popular entre las pequeñas y medianas empresas. Si bien es un poco más costoso inicialmente que las unidades USB, sigue siendo más barato que el hardware de cinta y ofrece una buena variedad de opciones de restauración para los usuarios.

Como la mayoría de las unidades USB, RDX es básicamente un disco duro SATA, pero está en un cartucho. Por extraño que pueda parecer, creo que una gran parte

de su atractivo para los usuarios es que simplemente les resulta más tranquilizador ver un cartucho de expulsión, listo para ser llevado fuera de las instalaciones.
Curiosamente, sin embargo, Windows no los ve de la misma manera como una unidad USB, sino que aparecen en el sistema operativo como un soporte óptico emulado, un poco como una unidad de DVD haría. Una consideración a causa de esto, es que se necesita para utilizar la opción de «contenedor de datos » especialmente si desea restaurar datos o realizar copias de seguridad incrementales (a diferencia de copias de seguridad completas cada vez).

Almacenamiento Conectado en Red (NAS)

Para proveer el almacenamiento en trama es necesaria una LAN o WAN, además de un dispositivo de almacenamiento dedicado y diseñado para esta infraestructura; su propósito es proporcionar a los usuarios un sistema de servicio de acceso e intercambio de información. El almacenamiento en red se caracteriza por el depósito masivo de datos, lo que incluye intercambio de datos limitados, fiabilidad y seguridad en los datos, y así como el simplificado y unificado en la gestión de datos. Aunque su principal bondad es la capacidad de expansión, donde se proporcionan tasas de transmisión de la información de acuerdo al volumen de datos. Las conexiones SAN y NAS son ejemplos claros del almacenamiento en red; las analizamos a continuación.
El Almacenamiento Conectado en Red o *NAS* (del acrónimo *inglés Network Attached Storage*) es un dispositivo que se conecta a la red y provee un almacén de datos que permite a varios hosts acceder al mismo lugar de almacenamiento a través de una red IP. El espacio de almacenamiento se presenta en la red con un nodo dedicado a través de un servidor de archivos, aunque en sistemas recientes este dispositivo puede ser un dispositivo inmerso en la red . NAS y LAN están en la misma red física; por lo tanto, NAS depende de ciertas características de LAN. Para ello necesita un gran ancho de banda en red y de muy alta potencia de procesamiento del CPU: cuando no se cumplen estas condiciones, la red se congestiona y su rendimiento se reduce.

Con el servidor de archivos se gestiona la entrada y salida de datos en el disco duro; además, se regula el acceso entre varios clientes de red. El almacenamiento en NAS tiene dos características. En primer lugar, es la conexión física, puesto que se conecta el servidor de archivos directamente al equipo de almacenamiento y otro punto a la red, evitando así la carga de entrada y salida de datos en el servidor; en segundo lugar, técnicamente, se reducen los movimientos del brazo de la unidad de disco duro y, por lo tanto, se reduce el desgaste. Sin embargo, en esencia la estructura de este tipo de almacenamiento muestra que todavía es un equipo de servidor tradicional.

Los principales beneficios de NAS son la facilidad de comunicación entre una computadora y el sistema de almacenamiento en comparación con una conexión de computadora a computadora. El intercambio y recuperación de datos mediante una sola fuente de almacenamiento genera menos errores, menos trabajo al tratar de mantener copias de seguridad, y mayor precisión en la búsqueda de información. Estos sistemas son más seguros, porque en lugar de almacenar los datos en un solo disco duro distribuyen copias de los datos entre distintos discos duros que actúan como uno solo. Cuando un disco duro falla, se alerta al administrador de redes, y la información continúa estando disponible para todos los usuarios.

Todos sabemos que un disco duro dañado puede ser reemplazado por uno nuevo sin necesidad de que los usuarios lo perciban, ya que desde sus computadores continuarán trabajando normalmente: continuarán teniendo acceso a la red y, por lo tanto, a la información que necesitan. En esta misma línea un disco de gran tamaño puede ser más barato que varios discos de menor capacidad de espacio. El sistema NAS tiene ventajas tales como facilidad en la instalación, complementos o extensiones (*plugs*), precio, flexibilidad de conexión, fácil mantenimiento, seguridad de autenticación, administración de espacio en disco y escalabilidad. Así las cosas, NAS es una opción ideal para organizaciones pequeñas y medianas que buscan, de una manera simple y rentable, lograr el acceso de datos rápido en nivel de archivo para varios clientes.

En contraste, la escalabilidad se presenta como desventaja a causa de que la capacidad se limita por los equipos y dispositivos conectados; asimismo, NAS no

podrá ser integrado cuando no esté bien configurado, y gracias a esto el sistema de archivos no podrá formarse. También existe un inconveniente con las copias de seguridad: si se hacen en horas de mayor tráfico de datos, es seguro que el consumo de ancho de banda y rendimiento será limitado. Por esto, cuando el número de usuarios simultáneos no es muy grande, NAS sería una económica y racional elección, pero no es adecuado con aplicaciones de grandes bases de datos. En realidad, NAS tiene que ser visto como un equipo de almacenamiento auxiliar en una red, el cual está directamente conectado a una red usando un hub o switch, y comunicándose por medio del protocolo TCP / IP; sin duda, NAS está orientado al paso de mensajes y archivos, formato en el cual transmite los datos.

Respaldo y almacenamiento en la nube

A la inversa, la copia de seguridad fuera del sitio transmite copias de datos a una ubicación remota, que puede incluir el centro de datos secundario de una empresa o la instalación de colocación arrendada. Cada vez más, la copia de seguridad de datos fuera del sitio equivale al almacenamiento en la nube basado en suscripción como un servicio, que proporciona una capacidad escalable y de bajo costo y elimina la necesidad del cliente de comprar y mantener hardware de respaldo. A pesar de su creciente popularidad, la elección de la copia de seguridad como un servicio requiere que los usuarios cifren los datos y tomen otras medidas para salvaguardar la integridad de los datos.

El respaldo en la nube se divide en lo siguiente:

- **Almacenamiento público en la nube:** los usuarios envían datos a un proveedor de servicios en la nube, que les cobra una tarifa de suscripción mensual basada en el almacenamiento consumido. Hay tarifas adicionales por ingreso y egreso de datos. Amazon Web Services (AWS), Google Compute Engine y Microsoft Azure son actualmente los mayores proveedores de nube pública.
- **Almacenamiento en la nube privada:** se realiza un respaldo de los datos en diferentes servidores dentro del firewall de la compañía, generalmente entre un centro de datos local y un sitio de recuperación de desastres

secundario. Por esta razón, el almacenamiento en la nube privada a veces se denomina almacenamiento interno en la nube.

- **Almacenamiento híbrido en la nube:** una empresa usa almacenamiento local y externo. Las empresas suelen utilizar el almacenamiento en la nube pública de forma selectiva para el archivo de datos y la retención a largo plazo. Utilizan el almacenamiento privado para el acceso local y la copia de seguridad para un acceso más rápido a sus datos más críticos.

La mayoría de los proveedores de copias de seguridad permiten respaldar las aplicaciones locales en una nube privada dedicada, tratando de manera efectiva la copia de seguridad de datos basada en la nube como una extensión del centro de datos físico del cliente. También conocido como recuperación de desastres como un servicio (DRaaS), este campo de maduración permite a una organización arrendar espacio en los servidores de almacenamiento de un proveedor de servicios para la copia de seguridad centralizada y la gestión de datos de la línea de vida.

La copia de seguridad de datos de nube a nube es un enfoque alternativo que ha ido ganando impulso. Con este método, los datos de un cliente se copian de una plataforma de copia de seguridad en la nube a otra nube. También se refiere a las copias de seguridad basadas en la nube de datos almacenados en plataformas de software como servicio (SaaS).

Ante esta alternativa, es importante considerar sus ventajas y desventajas y estudiar de qué manera estas apoyan o difieren de las necesidades de la institución o grupo de investigadores.

Algunas de las ventajas son:

- Pueden realizar respaldos de datos de forma automática, según se programe
- No requieren la intervención directa de las personas en la realización de tareas manuales asociadas al respaldo
- Permite que se mantengan copias de los datos en otras locaciones
- Pueden incluir servicios de encriptado

Algunas de las desventajas son:

- La ubicación exacta de los servidores en lo que operan los servicios puede estar fuera de la jurisdicción del país en el que se ubica la institución

- La velocidad con la que se puede acceder a los datos dependerá del ancho de banda disponible
- Las condiciones de seguridad a las que estén sujetos los datos variará, pudiendo no estar encriptados (según las condiciones en que se ofrece el servicio)
- La migración a un nuevo sistema puede verse dificultada al trabajar en sistemas propietarios
- Deben considerarse aspectos contractuales que podrían condicionar aspectos como el acceso, uso y migración de los datos (por ejemplo: restricciones o costos de migración de un proveedor a otro; condiciones de finalización de servicios; derechos de propiedad intelectual asociados a la información, mecanismos de resolución de conflictos, entre otros.

1- Investiga una empresa de la comunidad, detalla los riesgos a los que se encuentran expuestos sus sistemas de información.

2- Define estrategias, métodos o tecnologías que ayuden a minimizar los riegos encontrados.

3- Elabora un plan de mantenimiento y respaldo óptimos y apropiados para la organización estudiada.

Bibliografía

- Stallings, W. (2004). Fundamentos de Seguridad en Redes. Aplicaciones y Estándares. Segunda Edición. Pearson Educación, S.A. Madrid.
- Daniel Sol Llaven. (2015). Sistemas Operativos. Panorama para la Ingeniería en Computación e Informática. Grupo Editorial Patria, S.A. México.
- Tanenbaum, Andrew S. (2003). Redes de Computadoras. Pearson Educación. México.
- Oz Effy. (2008). Administración de los Sistemas de Información. 5ª Ed. Cengage Learning Editores, S.A. México.
- Julio Gómez López, Oscar David Gómez López. (2011). Administración de sistemas operativos. Ediciones Ra-Ma. España.
- Herencia, José. (2011). Gestión de Documentos Electrónicos en Archivos Virtuales: Servicios en la Nube. Anuario Escuela de Archivología III. Universidad Nacional de Córdoba. ISSN 1852-6446.
- Cano A., Legañoa D., Cabrera I., Campillo I., (2012). Estructura del Sistema de Gestión Integral de Documentos de Archivo (SiGeID). Colombia. Revista Interamericana de Bibliotecología, vol 35, núm 2, pp. 149-161.
- CARRETERO Pérez, Jesús, Sistemas operativos, una visión aplicada, México, Mc. Graw-Hill, 2000