# I. Administración de sistemas operativos

La administración de sistemas de cómputo en general y sistemas operativos en particular consiste en la planeación, instalación y mantenimiento de los recursos y servicios que necesitan los usuarios de un sistema de cómputo para satisfacer adecuadamente sus necesidades

Algunas funciones como la instalación y configuración del S.O., adición de nuevos usuarios, realización de respaldos, mantenimiento de la seguridad, configuración del acceso a Internet y otros, son solo parte del trabajo. Existen requisitos no técnicos muy significativos para ser buen administrador de sistemas, especialmente en términos de planeación, organización e incluso relaciones humanas.

Conforme los sistemas de cómputo se hacen más importantes para el funcionamiento de las empresas, los administradores deben entender mejor al tipo de sistemas que manejan, a la gente que los utiliza y a la naturaleza del negocio que se desarrolla a su alrededor. Una habilidad clave es la planeación, ya que debido a la velocidad con la que los sistemas crecen y se expanden en las organizaciones, el tratar de diseñar e implementar una modificación "al vuelo" difícilmente funciona.

**Funciones del administrador del sistema operativo**

Estas funciones pueden dividirse generalmente en dos categorías: soporte a usuarios y soporte al sistema

**Soporte a usuarios**

- **Creación de cuentas de usuarios**.- Por ejemplo, en el caso de UNIX, el trabajo puede consistir en:

    Añadir el usuario al archivo `/etc/passwd` y/o `/etc/shadow` , asignándole un número único de usuario, un grupo al cual pertenece, un directorio HOME y un shell de entrada

    Crear el directorio HOME, con los permisos adecuados para que el usuario pueda manejar sus archivos

    Copiar un "esqueleto de archivos" genérico, que le den al usuario un ambiente básico para trabajar, con las trayectorias (paths) y variables de ambiente necesarias para correr aplicaciones y utilerías y

    Registrar al nuevo usuario en la red del sistema, tales como NIS y NFS si es que el usuario requiere acceso a sistemas de archivos remotos.

- **Proporcionar soporte**.- Proporcionar a los usuarios documentación y soporte es una tarea que puede convertirse en un dolor de cabeza. (Se dice que el mejor administrador es invisible y, al mismo tiempo, está siempre a la mano).

    La idea de enseñar a los usuarios la manera de resolver sus problemas en vez de esperar que el administrador lo haga por ellos es útil, pero hay que estar conscientes de que no puede aplicarse por igual a todos los tipos de usuarios. Sin embargo es útil ofrecer una cuenta de correo y/o una página Web para soporte y, de esta forma, enseñar a los usuarios interesados la manera de no depender tanto del administrador

**Soporte al sistema**

Es la otra mitad del trabajo. Los sistemas deben ser construidos, respaldados, actualizados y, desde luego, arreglados:

- **Adición de nodos**.- Es una tarea frecuente para sistemas con redes y es una de las partes que se benefician más si existe una buena planeación. No todos los sistemas son creados igual, y una buena planeación depende de los objetivos que desean cubrirse con cada sistema. Las estaciones de trabajo deben tener roles bien definidos y estar configuradas de acuerdo a esos roles.

Algunas preguntas que para este efecto debe hacerse el administrador son:

¿Los usuarios deben poder accesar todo el sistema o sólo parte de él? ¿Los usuarios necesitan accesar varios sistemas simultáneamente? ¿Existen sistemas que los usuarios nunca deben poder accesar?

¿Qué sistemas de archivos podrán accesar las estaciones de trabajo? ¿Puede automatizarse el proceso para accesarlos?

¿Qué servicios como telnet, ftp y correo entre otros estarán disponibles para los usuarios en las estaciones? ¿Se justifica la existencia de cada servicio?

Responder estas preguntas permiten generar un perfil para cada estación, lo que las hace más fáciles de construir y mantener y menos complejas.

- **Respaldos**.- Los archivos son los elementos más importantes para almacenamiento de información y necesitan ser conservados para evitar pérdidas importantes de tiempo y trabajo.

  Todos los sistemas operativos proporcionan utilerías para respaldo de información en discos magnéticos, y algunos también en cintas magnéticas y discos ópticos y magneto-ópticos (tar, cpio, msbackup, etc). La mayoría de estas herramientas son simples y rudimentarias, pero con un poco de práctica pueden implementarse rutinas de respaldo automáticas o casi automáticas que se activen en momentos determinados del día. Sin embargo, actualmente existen muchas herramientas adicionales que facilitan la creación de respaldos, sobre todo si se utiliza una interfaz gráfica.

  Diseñar una política de respaldos es tan importante como escoger una herramienta para hacerlo. Respaldar diariamente el sistema completo es inaceptable, ya que puede tardar demasiado y requerir mucho espacio. Además generalmente son pocos los archivos dañados o perdidos que requieren restaurarse. De esta manera que es importante hacerse algunas preguntas para diseñar una estrategia de respaldos:

  ¿Los usuarios tienen archivos importantes que se modifiquen diariamente?

  ¿Los usuarios almacenan su información en directorios centralizados comunes, o deben copiarse desde sus lugares de origen a través de la red?

  ¿Si sólo un archivo requiere restauración, ésta debe ser rápida? ¿El medio de respaldo disponible, permite la recuperación de archivos particulares?

  ¿Qué tan frecuentemente y durante cuánto tiempo los usuarios están fuera del sistema? (Es mucho mejor hacer los respaldos cuando el sistema no se está utilizando)

- **Carga del sistema y desempeño**.- Son responsabilidades directas del administrador, y otra de las áreas que se benefician más de la correcta planeación.

  El monitoreo diario de estadísticas de uso del sistema es una buena medida, especialmente en sistemas de “misión crítica” y aquellos con los que los usuarios interactúan de manera regular, como Web servers y manejadores de bases de datos. Esto puede lograrse generalmente de manera automática con macros o scripts del sistema.

Algunos aspectos importantes a monitorear son:

- Utilización del disco (`du, df`)
- Uso del CPU (`top, vmstat`)
- Espacio de intercambio de memoria virtual (swap)
- Memoria física

Las herramientas útiles para monitoreo son diversas. Por ejemplo, en el caso de UNIX tenemos:

El shell.- Permite la construcción de programas con construcciones sofisticadas, como ciclos, y proporciona operadores de comparación como igual-que, mayor-que o menor-que. Puede ser usado para realización de respaldos, creación de cuentas de usuarios y recolección de estadísticas entre otros.

Perl y otras herramientas de automatización.- Perl (Practical Extraction and Report Languaje) es un lenguaje interpretado, lo que lo hace independiente de plataformas, sencillo y ampliamente difundido. Permite hacer programas que antes sólo podían programarse en C y tiene acceso directo a comandos de UNIX. Algunos ejemplos son:

- Analizar de archivos de registro y enviar una alerta al administrador vía e-mail o a la consola
- Convertir automáticamente las estadísticas del sistema en páginas Web
- Automatizar la administración de cuentas de usuarios, los respaldos y la creación de páginas HTML
- Comunicarse con otras aplicaciones a través de la red

Otro lenguaje ampliamente utilizado es TCL/TK, que permite usar un ambiente gráfico, y en el que la mayoría de las utilerías administrativas de Linux RedHat están programadas.

**Seguridad**

Un problema de gran relevancia en los sistemas de cómputo multiusuario, es el asegurar de alguna manera que la información que almacenan es consistente y privada, y que continuará siéndolo a través del tiempo. Dos tipos de eventualidades que pueden hacer que este objetivo no se consiga son las descomposturas físicas del sistema y las violaciones a la seguridad.

Es responsabilidad del administrador del sistema establecer una política de seguridad e implementarla correctamente. Existen diversos enfoques para resolver el problema de la seguridad, pero en general, todos parten de la obtención de información completa del sistema en los siguientes aspectos:

Hardware.- Deben obtenerse referencias precisas de la configuración de cada máquina: fabricante, modelo y número de serie de cada estación, concentrador, ruteador, tarjeta de red y demás dispositivos. Idealmente deberían tenerse relaciones de la cantidad de memoria, capacidad de disco y especificaciones de la red.

Software.- Lista de todos los tipos de software de red que pretendan ejecutarse y sus números de versión.

Protocolos.- Información de los protocolos de comunicaciones que utilice el sistema. Se debe tratar de establecer prioridades de acuerdo a la función de cada estación y limitar la cantidad de protocolos instalados.

Alcance.- El número máximo de estaciones que tendrá el sistema, su localización física, los segmentos que conforman la red, y demás detalles relevantes.

La política de seguridad debe incluir aspectos tales como la clasificación de la información que se maneja de acuerdo a su nivel privacidad, los costos que implicaría a la organización la fuga de información en términos económicos y de tiempo de trabajo y estar consciente de las implicaciones legales y/o judiciales de una falla en el cumplimiento de dicha política.

También es necesario comprender que no existe un sistema que se pueda considerar cien por ciento seguro.

El empleo de esquemas de seguridad basados en claves de usuario y password está ampliamente difundido. A través del nombre de usuario se lleva un control de la cantidad y tipo de recursos a los que el usuario tiene acceso. Sin embargo este esquema es relativamente fácil de violar, por lo que se han desarrollado estructuras más complejas que van desde la autentificación de los usuarios hasta el encriptamiento de la información que viaja en la red.

Kerberos es un ejemplo de sistema de autentificación. Cuando el usuario se da de alta en un servidor, verifica su identidad y le entrega un “boleto”, a través del cual podrá validar constantemente esta identidad sin tener que transmitir el password. Estos boletos contienen información encriptada sobre los privilegios del usuario, los grupos a los que pertenece y el tiempo de expiración del boleto entre otros.

Cada vez que el usuario realiza alguna tarea, se verifica la autenticidad de estos boletos y después se revisan los privilegios del usuario antes de permitirle la ejecución. Como los boletos sólo son válidos durante un tiempo determinado, un boleto robado no sirve si se intenta utilizar después.

El encriptamiento es un complemento de la autentificación y permite cifrar los mensajes originales antes de enviarlos con el uso de una clave:

Mensaje encriptado = {Mensaje original} Clave

El mensaje puede volverse a su estado original en el receptor si se conoce el procedimiento inverso al de encriptamiento y la clave original. También existen métodos que utilizan varias claves en vez de una, lo que los hace más difíciles de violar.

El administrador es el encargado de asignar los nombres de usuario y passwords, así como establecer el método de autentificación y de encriptamiento en caso de ser requeridos, además de exigir actualizaciones periódicas de passwords.