Tema 1: Introducción a la administración de sistemas

Administración de Sistemas e Redes

Tomás Fdez. Pena

tf.pena@usc.es

Índice

1. Introducción a la asignatura

1.1. La figura del administrador de sistemas

- El administrador de sistemas es quien tiene la capacidad y la responsabilidad de establecer las acciones, procedimientos y normas para conseguir:
  - asegurar que el sistema funcione correcta y eficientemente, y

    - asegurar que todos los usuarios pueden usar el sistema de manera fácil y sin problemas
- Tarea esencial, dado el incremento en la complejidad de los sistemas y redes

1.2. Objetivos de la asignatura

- Adquirir competencias de un Administrador de Sistemas a nivel intermedio
    - Facilidad de uso de la mayor parte de los aspectos de la administración de sistemas GNU Linux/UNIX
    - Conocimiento de administración de redes
    - Capacidad de entender y escribir scripts de administración
    - Capacidad de identificar tareas que requieran automatización y automatizarlas
    - Capacidad de resolver problemas rápida y completamente

1.3. ¿Por qué UNIX/GNU Linux?

- UNIX tiene una larga historia en la industria y la educación
- UNIX/GNU Linux es popular a nivel de empresa
- Es independiente del hardware
- GNU Linux es abierto y gratuito
- GNU Linux proporciona prácticamente todo el software necesario para un sistema completo

¿Por qué no Windows?

- Dependencia de una sola empresa
- Es caro
- No es completo
- Es cerrado
- Oculta su complejidad
- Conociendo Linux es fácil aprender otros SO

1.4. Información oficial

- 6 ECTS $\longrightarrow$ 5 horas expositivas/45 laboratorio
- Asistencia obligatoria a clases de laboratorio
- Evaluación: 60 % examen teoría/40 % evaluación prácticas
- Apuntes disponibles en el CV o en http://persoal.citius.usc.es/tf.pena/ASR/
- Profesorado:
  - Teoría: Tomás Fernández Pena
  - Prácticas: Francisco Argüello Pedreira

Información completa:
www.usc.es/gl/centros/etse/materia.html?materia=85056&ano=66

1.5. Relación con otras asignaturas

Administración Avanzada de Sistemas e Redes. Optativa, trata aspectos de monitorización y optimización de servidores, virtualización, gestión de redes y administración de servicios (web, e-mail, etc.).

Seguridade Informática. Obligatoria, cubre aspectos de seguridad en redes (cortafuegos, VPNs, IDs, etc.).

Enxeñaría de Computadores Obligatoria, instalación y configuración de centros de procesado de datos e instalaciones informáticas de tamaño medio/grande (servidores, virtualización y consolidación, redes de almacenamiento, backups, etc.).

Administración de Bases de Datos. Optativa, trata la administración de sistemas de gestión de bases de datos (instalación y gestión, seguridad, backups, etc.).

2. Tareas de un administrador de sistemas

Tareas comunes:

- Administrar el hardware de los sistemas
- Administrar las aplicaciones instaladas

- Administrar usuarios
- Comprobar el buen funcionamiento del sistema
- Contabilizar el uso de recursos por parte de los usuarios
- Administración de la seguridad
- Mantenimiento de la documentación
- Soporte técnico a usuarios

Tareas específicas dependen del entorno donde desarrolle su trabajo el administrador, incluyendo tipos de usuarios, hardware/software disponible, políticas de gestión, etc.

1. **Entorno de trabajo**
   - Entorno de trabajo (empresa, administración pública, etc.) compuesto de :
     - usuarios (de 10 a 1000s),
     - recursos materiales (posiblemente operando 24x7),
     - información (software, archivos, etc.)
     - políticas de gestión
2. **Usuarios**
   - Algunas características:
     - número,
     - experiencia (o no) en el uso de sistemas informáticos,
     - tipo de trabajo,
     - responsabilidad o irresponsabilidad
3. **Hardware/Software**
   - Los ordenadores, software, redes, impresoras, etc. influyen en el tipo de trabajo del administrador
     - número y complejidad,
     - una o varias redes,
     - sistemas homogéneos o heterogéneos, corriendo el mismo o diferente SO y software de aplicaciones:
       - PCs tradicionales

        - servidores sin monitor
        - sistemas sin interfaz gráfico
        - sistemas sin disco
        - sistemas con varias CPUs (SMP, clusters, etc.)
        - ...

4. **En cualquier caso**

    - El administrador es un instrumento para facilitar la vida a los usuarios, no para complicársela:
        - Tener siempre presente el espíritu de servicio
        - Informar a los usuarios de los cambios en el sistema que les afecten, personalmente o mediante herramientas de comunicación, sin llegar a saturar
        - Ayudar en los problemas que surjan a los usuarios
        - Atender sus quejas con educación, pero ser capaz de imponer su autoridad cuando sea preciso
        - No olvidar que los usuarios no son expertos y su conocimiento informático puede ser nulo

2.1. Principales tareas

Cuatro categorías:

- operaciones diarias
- hardware y software
- interacción con los usuarios
- organización y planificación

1. **Operaciones diarias**

    - Tareas que deben realizarse regularmente, por ejemplo:
        - Añadir y borrar usuarios
        - Monitorizar el sistema:
            - uso de recursos: CPU, memoria, discos, etc.
            - actividades irregulares de los usuarios
            - problemas inesperados
        - Realizar copias de seguridad

- Muchas de esas tareas pueden (y deberían) ser automatizadas
  - se evita *reinventar la rueda*
  - simplifica el trabajo
  - permite delegar en otros

2. Hardware y software

- Algunas tareas relacionadas con hardware y software:
  - evaluación y compra,
  - instalación y mantenimiento,
  - prevención de problemas,
  - actualización de hardware y software,
  - eliminación y migración de sistemas antiguos

3. Organización y planificación

- El administrador debe ser capaz de anticiparse a los problemas (proactividad)
  - necesidad de organización y planificación
- Elementos a tener en cuenta:
  - documentación: para el administrador, los usuarios y la dirección
  - gestión del tiempo de trabajo
  - planificación a medio y largo plazo
  - actualización de conocimientos
  - automatización de actividades repetitivas

4. Documentación

- Posiblemente la tarea más aburrida, pero una de las más importantes,
  - documentación acerca de los detalles de cada sistema particular:
    - localización, detalles de compra, ...
    - software instalado, usuarios, ...
    - ficheros de configuración, ...
  - etiquetado del hardware
    - información sobre el nombre, IP, MAC, etc. de cada sistema particular
  - libro de cambios en los sistemas
    - modificaciones en los ficheros de configuración, actualizaciones, ...

- informes sobre las tareas realizadas
  - facilitan resolver un problema cuando ocurre por segunda vez
- documentación para usuarios sobre uso de los sistemas

2.2. Fuentes de información para el administrador

Una parte esencial de la tarea del AS es diagnosticar y resolver problemas

Para resolver un problema debemos:

1. mantener la calma
2. consultar las fuentes de información disponibles:
   - conocer los sitios donde mirar,
   - antes de preguntar, intentar ver si el problema ya está descrito,
   - al preguntar, ser educado, conciso e informativo
3. registrar la solución
4. contribuir a la comunidad

No podemos conocer todo lo necesario para resolver todos los problemas, pero si debemos saber donde acudir en busca de información.

Fuentes de información:

- Asociaciones profesionales y grupos de usuarios:
  - Galicia: OSL-CIXUG, GPUL, Ghandalf, GALPon, etc.
  - España: Hispalinux
  - Internacional: USENIX, LISA, ACM, IEEE Computer, etc.
- Libros y revistas:
  - En general, referenciados por el nombre RTFM (Read The F. Manual)
  - Multitud de libros y revistas sobre UNIX/Linux, algunas online como LinuxGazette, LinuxFocus o OpenSource Subnet
  - A destacar la colección de O'Reilly
- Internet
  - Es la principal fuente de información para administradores y usuarios

Fuentes en Internet

En Internet podemos encontrar:

- software,
- información (documentación, guias, HOWTOS, etc.)
- foros de discusión

Software

- paquetes RPM: rpmfind.net
- paquetes Debian: www.debian.org/distrib/packages
- paquetes en código fuente: sourceforge.net
- ...

Documentación

- The Linux Documentation Project (www.tldp.org) mantiene guías, FAQs, HOWTOs

  HOWTO Documentos sobre aspectos específicos de Linux, por ejemplo:
  - *Partition HOWTO*, *NFS-HOWTO*, *Network Install HOWTO*, etc.
- Howtoforge (www.howtoforge.com) tutoriales varios
- Documentación de empresas y distribuciones, por ejemplo:
  - IBM developerWorks, por ejemplo preparación para las certificaciones LPI[1]
  - Documentación de Red Hat (www.redhat.com/docs/)
  - Documentación de Debian (www.debian.org/doc/index.en.html)
  - Documentación de Ubuntu (help.ubuntu.com)

[1]LPI: Linux Professional Institute: organización sin animo de lucro que proporciona certificaciones para administradores Linux

Foros de discusión

- Grupos de noticias:
  - instalación y administración:
    - comp.unix.admin, comp.os.linux.setup,...
  - redes:
    - comp.os.linux.networking,...
  - seguridad:
    - comp.security.unix, comp.os.linux.security,...
  - varios:
    - comp.unix.misc, comp.os.linux.misc, ...
  - para buscar algo concreto: groups.google.com
- Listas de correo:
  - existen listas de correo para multitud de tópicos:
    - listas de correo de Debian (www.debian.org/MailingLists)
    - listas de correo de GNOME (mail.gnome.org), o KDE (lists.kde.org)
    - ...
  - otros foros:
    - LinuxForums
    - LinuxQuestions
    - StackOverflow
    - ...

Otras fuentes de información

- Soporte y documentación oficial de las distribuciones:
  - Ubuntu, Debian, RedHat, ...
  - Impresoras: OpenPrinting, laptops, etc.
  - ...
- Compatibilidad hardware de Linux:
  - www.linuxhardware.net
  - Impresoras: OpenPrinting, laptops, etc.
  - ...
- Trucos, ayuda,

    - Linux Help
    - Just Linux
    - ...
- Seguridad
    - Kriptopolis: Información y noticias sobre criptografía y seguridad (en castellano)
    - CERT (de la Carnegie Mellow University): anuncios de seguridad, parches, etc.
    - SecurityFocus.com: especializado en noticias e información sobre seguridad
    - SANS: *the System Administration, Networking, and Security Institute*
    - ...
- Noticias, información, comentarios, enlaces, etc.
    - UGU: Unix Guru Universe; material para administradores UNIX
    - SlashDot: noticias para *nerds*
    - Freecode: información sobre aplicaciones *open source*
    - LinuxPlanet: discusiones, foros, tutoriales, etc.
    - Linux Today: actualidad Linux
    - Linux.org, Linux.com: noticias, foros,...
    - Linux Foundation: promueve el uso de Linux
    - kernel.org: Linux Kernel Archives
    - Distrowatch: información sobre distribuciones Linux y BSD
    - ...

3. Políticas y estándares

Políticas de gestión

- Definen el qué, por qué y cómo hacer las cosas en la organización
    - determinan el tipo de uso que los empleados pueden hacer de los sistemas, p.e.
        - derechos de acceso a los recursos,
        - limites en el uso de recursos (disco, CPU, etc.),

        - ¿puede el AS acceder al e-mail de los usuarios?
    - Normalmente, las políticas de gestión son responsabilidad de la gerencia o dirección técnica de la organización
        - el administrador debe respetar y hacer respetar esas políticas
        - no inventar políticas de uso de recursos que contradigan las políticas generales
    - La obediencia no debe ser ciega: si se considera que una política no se puede implantar o se puede mejorar, hay que dialogar con los superiores
    - Junto con las políticas, se debe establecer un sistema de penalizaciones

3.1. Políticas y procedimientos

Importante disponer de un conjunto amplio de políticas y procedimientos

- Políticas: documentos que definen requerimientos o reglas (p.e. cuándo y de qué se hacen backups), no suelen modificarse a menudo
- Procedimientos: documentos que explican como llevar a cabo los requerimientos (p.e. cómo se hacen los backups), deben adaptarse continuamente

Políticas

Necesidad de documentos de políticas escritas y firmadas

- Políticas de los servicios administrativos
- Derechos y responsabilidades de los usuarios
- Políticas aplicables a los administradores de sistemas
- Políticas de usuarios temporales

Todos los usuarios deberían firmar un documento de conformidad Ejemplos de políticas

- Normativa de la USC
- Ejemplo de la Universidad de California y el Centro de Supercomputación de San Diego

Políticas de seguridad

Toda política está relacionada con la estabilidad y seguridad del sistema

- debe quedar claro qué proteger y las prioridades

Necesidad de obtener un equilibrio

- Servicios ofrecidos vs. seguridad proporcionada (más servicios = menos seguridad)
- Facilidad y comodidad de uso vs. seguridad (seguridad=1/comodidad)
- Coste de la seguridad vs. riesgo (coste) de las pérdidas

Necesario crear guías de seguridad

- Ver ejemplo en el Centro de Supercomputación de San Diego

Necesaria una política de recuperación de desastres

- Ver libro base, sección 32.8

Procedimientos

Recetas para realizar determinadas tareas

- Añadir o dar de baja un host
- Añadir o dar de baja a un usuario
- Actualizar un sistema
- Realizar copias de seguridad de los sistemas
- Realizar apagados de seguridad
- etc.

Recetas por escrito y siempre disponibles

- Pueden tomar la forma de scripts comentados
- Un nuevo administrador debe ser capaz de entenderlas rápidamente

3.2. Estándares y recomendaciones

Existen estándares para la gestión correcta de las infraestructuras de IT y la seguridad

- Esquemas de certificación para valorar las instalaciones

Estándares relacionados con la seguridad

1. ISO 27002 (anteriormente ISO 17799, basado en el británico BS 7799-1)
   - Recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización
   - No es una norma tecnológica
     - proporciona buenas prácticas neutrales con respecto a la tecnología y a las soluciones disponibles en el mercado
   - Forma parte del grupo de estándares ISO 27000
   - Estándares relacionados:
     - ISO 27001, especifica requisitos para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información consistente con ISO/IEC 27002, reemplaza al BS 7799-2
2. *Standard of Good Practice*
   - Documentación detallada que identifica buenas prácticas en seguridad de la información
   - Creado por el Information Security Forum
3. RFC 2196, *Site Security Handbook* y RFC 2504, *Users' Security Handbook*
   - Documento práctico con recomendaciones sobre aspectos de seguridad, políticas de usuarios y procedimientos
   - Proporciona una visión general sobre la seguridad de la información, incluyendo seguridad de red, respuesta a incidentes o políticas de seguridad

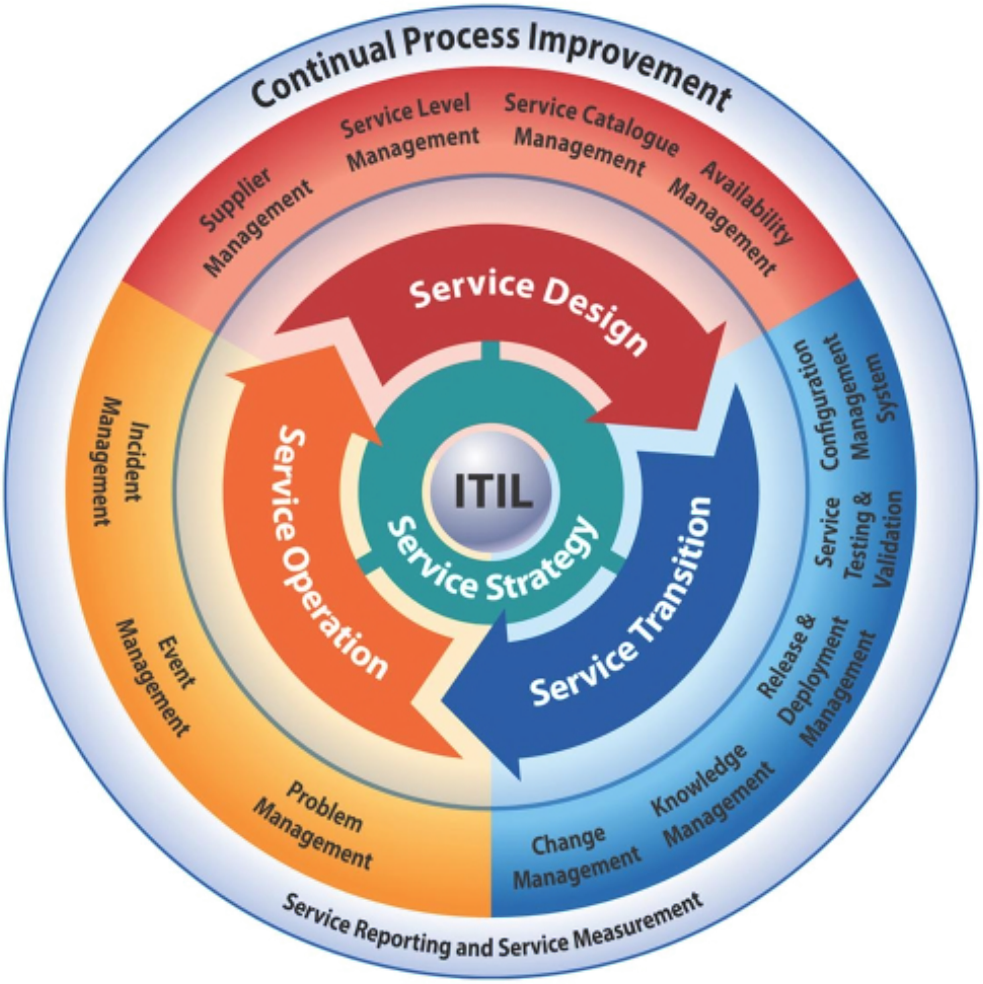
Otros estándares

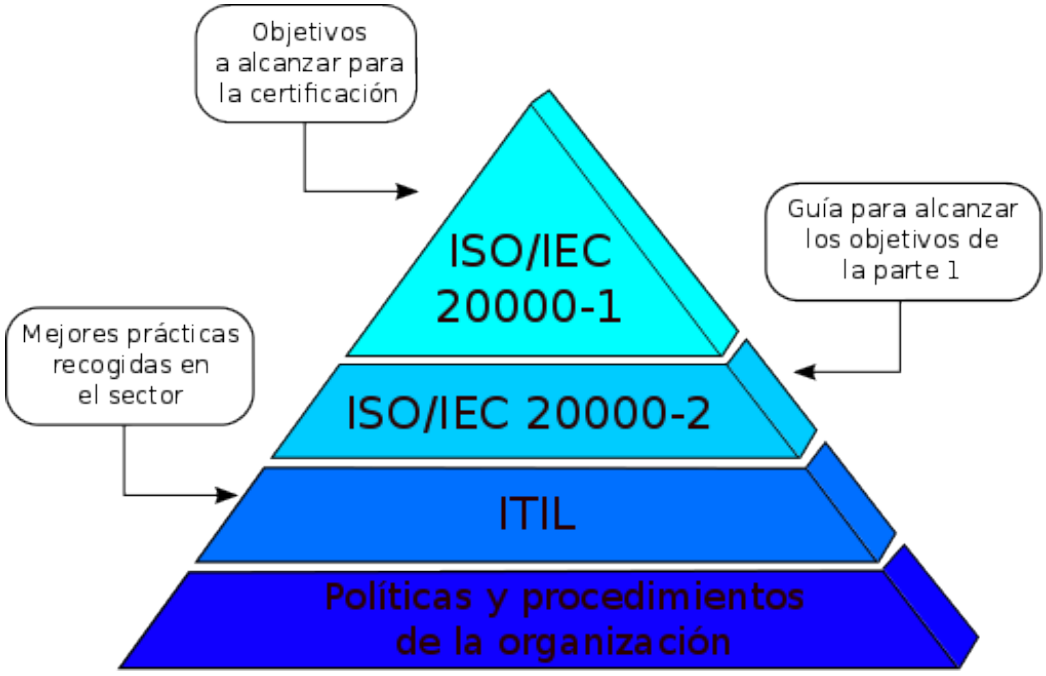
1. ISO/IEC 20000

   - Estándar internacional en gestión de servicios de Tecnologías de la Información
   - Basado en el estándar británico BS 15000, desarrollado en 2005 y revisado en 2011/12
   - Tiene 5 partes, las más importantes son la
     - ISO/IEC 20000-1:2011, define los requerimientos necesarios para garantizar una entrega de servicios de TI con calidad aceptable para todos los clientes
     - ISO/IEC 20000-2:2012, guía de implementación de los sistemas de gestión de servicios, para alcanzar los requerimientos de la ISO/IEC 20000-1

2. ITIL (*Information Technology Infrastructure Library*)

   - Conjunto de documentos de buenas prácticas para la gestión de servicios de TI
   - Proporciona un marco de trabajo adaptable de buenas prácticas para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI
   - ITIL v3 (mayo 2007, actualizado en julio 2011) consta de 5 libros: *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation* y *Continual Service Improvement*
   - Cuatro niveles de certificación ITIL v3 para profesionales: Foundation, Intermediate, Expert y Master (no certificación para organizaciones)


Continual Process Improvement
Service Level Management
Service Catalogue Management
Availability Management
Supplier Management
Service Design
Service Operation
Service Transition
Service Strategy
ITIL
Incident Management
Event Management
Problem Management
Change Management
Knowledge Management
Release & Deployment Management
Service Testing & Validation
Configuration Management System
Service Reporting and Service Measurement



3. COBIT (*Control Objectives for Information and related Technology*)

   - Marco de trabajo de buenas prácticas para TI
   - Desarrollado por la Information Systems Audit and Control Association
   - Última versión: COBIT 5 (junio 2012)
   - Incluye 34 objetivos de alto nivel, que cubren 215 objetivos de control categorizados en 4 dominios: planificación y organización, adquisición e implementación, entrega y soporte, y monitorización y evaluación.