UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
" ACATLAN "

FALLA DE ORIGEN

CONTROL DE ACCESO LOGICO EN EL SISTEMA IBM AS / 400

T E S I N A

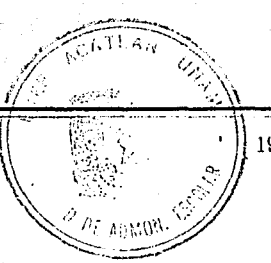
QUE PARA OBTENER EL TITULO DE

LICENCIADO EN MATEMATICAS APLICADAS Y COMPUTACION

P R E S E N T A :

JUAN MANUEL ACEVES MERCENARIO

Asesor: Fis. Mat. Jorge Luis Suárez Madariaga



MEXICO, D F. 1995

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

DERECHOS RESERVADOS © PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis está protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

UNIVERSIDAD NACIONAL AVENOMA DE MEXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES "ACATLAN"

DIVISION DE MATEMATICAS E INGENIERIA
PROGRAMA DE ACTUARIA Y M.A.C.

SR. JUAN MANUEL ACEVES MERCENARIO
Alumno de la carrera de M.A.C.
P r e s e n t e .

Por acuerdo a su solicitud presentada con fecha 6 de octubre de 1994, me complace notificarle que esta Jefatura tuvo a bien asignarle el siguiente tema de Tesina: "CONTROL DE ACCESO LOGICO EN EL SISTEMA IBM AS/400", el cual se desarrollará como sigue:

PROLOGO
CAP. I Consideraciones Preliminares
CAP. II Visión General del AS/400
CAP. III Terminología Básica del AS/400
CAP. IV Características de Seguridad del AS/400
CAP. V Niveles de Seguridad
CAP. VI Perfiles de Usuario
CONCLUSIONES
BIBLIOGRAFIA

Asimismo, fué designado como Asesor de Tesina el F.M. JORGE LUIS SUAREZ MADARIAGA, Profesor de esta Escuela.

Ruego a usted tomar nota que en cumplimiento de lo especificado en la Ley de Profesiones, deberá presentar servicio social durante un tiempo mínimo de seis meses como requisito básico para sustentar examen profesional así como de la disposición de la Coordinación de la Administración Escolar en el sentido de que se imprima en lugar visible de los ejemplares de la tesina el título del trabajo realizado. Esta comunicación deberá imprimirse en el interior de la misma.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Acatlán, Edo. Méx. noviembre 18 de 1994.

ACT. LAURA MAY RIVERA BECERRA
Jefe del Programa de Actuaría
y M.A.C.

cg'

JEFATURA DEL PROGRAMA DE ACTUARIA Y MATEMATICAS APLICADAS Y COMPUTACION

A mi esposa Luisa y a mi hija Brenda, las dos bellas mujeres sobre las que gira mi existencia, mi tesoro más preciado.

A mis padres Manuel y Norma, por su inagotable cariño y apoyo

A mis hermanos Jorge, Emiliano y Normita

A mi futuro hijo

Las siguientes personas han contribuido grandemente en mi formación personal y profesional. A todas ellas mi agradecimiento y admiración:

Jorge Mercenario
Rosario Cervantes
Manuel Aceves de la Peña
Nina Aceves
Oscar Mercenario
Raquel Trujillo
Vida Mercenario
Irma Mercenario
Javier Manero
Jorge Aceves P.
Javier Aceves
Laura Aceves
Jorge Romero
Luis Humberto Sánchez C.
María Luisa Sandoval
César Sánchez
Charles De Olden
Javier Soni
Carlos Moreno
César Javier Lara
Jorge Green
Luis Molina
Carlos Fischer
Miguel Angel Valera
Tulio Demicheli
Rubén Rojas
César Feerman
Oscar Feerman
Mauricio Solórzano
Carlos Alcázar
Manuel Riestra
Juan Jorge Farías
Hiroshi Matzura
Héctor Cruz

Indice

Indice

Prólogo vi

1. Consideraciones Preliminares 1
   1.1 Componentes de la Seguridad Lógica 2
   1.2 Control de Acceso Lógico 4

2. Visión General del AS/400 7
   2.1 Antecedentes 8
   2.2 Arquitectura 12
      2.2.1 Máquina de Alto Nivel 12
      2.2.2 Orientación hacia Objetos 14
      2.2.3 Almacenamiento de un Solo Nivel 14
      2.2.4 Jerarquía de Microprocesadores 15
      2.2.5 OS/400 16

3 Terminología Básica del AS/400 18
   3.1 Lenguaje de Control 19
   3.2 Objetos 19
   3.3 Asignación y Direccionamiento de Espacio de Almacenamiento 21
   3.4 Bibliotecas 22

3.5 Archivos 22
3.5.1 Archivos Físicos 23
3.5.2 Archivos Lógicos 24
3.6 Diccionarios de Datos 25
3.7 Trabajos 25
3.8 Colas de Trabajo 25
3.9 Subsistemas 26
3.10 Descripciones de Configuración 26
3.11 Colas de Salida 27
3.12 Salidas del Sistema 27
3.13 Programas y Comandos 28

4. Características de Seguridad del AS/400 29
4.1 Perfiles de Usuario 30
4.2 Autoridades Especiales 30
4.3 Clases de Usuario 41
4.4 Perfiles de IBM 33
4.5 Perfiles de Grupo 33
4.6 Capacidades Limitadas 34
4.7 Autoridades Específicas 34
4.8 Portadores de Autoridad 38
4.9 Autoridad Pública 38
4.10 Propiedad Individual y Grupal 38
4.11 Listas de Autorización 39

4.12 Búsqueda de Autorizaciones 40
4.13 Autoridad Adoptiva 41
4.14 Valores del Sistema 42
4.15 Administración de Passwords 42
4.16 Uso de Comandos 47
4.17 Uso de Terminales 47

5. Niveles de Seguridad 48
5.1 Nivel de Seguridad 10 50
5.2 Nivel de Seguridad 20 50
5.3 Nivel de Seguridad 30 51
5.4 Nivel de Seguridad 40 52
5.4.1 Uso de Interfases no Soportadas 53
5.4.2 Uso de Instrucciones Restringidas 54
5.4.3 Protección de Descripciones de Trabajos 54
5.4.4 Sign-on sin Password 55
5.4.5 Protección de Almacenamiento por Hardware 55
5.4.6 Validación de Programas Restaurados . . 55

6. Perfiles de Usuario 57
6.1 Roles del Perfil de Usuario 58
6.2 Campos del Perfil de Usuario 58
6.2.1 Nombre del Perfil de Usuario (USRPRF) . 59

6.2.2 Password (PASSWORD) 59

6.2.3 Expiración de Passwords (PWDEXP) . . . 61

6.2.4 Status (STATUS) 61

6.2.5 Clase de Usuario (USRCLS) 62

6.2.6 Biblioteca Actual (CURLIB) 63

6.2.7 Programa Inicial (INLPGM) 64

6.2.8 Menú Inicial (INLMNU) 65

6.2.9 Capacidades Limitadas (LMTCPB) 66

6.2.10 Texto (TEXT) 67

6.2.11 Autoridad Especial (SPCAUT) 68

6.2.12 Desplegado de Información de Sign-on (DSPSGNINF) 68

6.2.13 Intervalo de Expiracion del Password (PWDEXPITV) 69

6.2.14 Limitar Sesiones de Dispositivo (LMTDEVSSN) 70

6.2.15 Perfil de Grupo (GRPPRF) 70

6.2.16 Propietario (OWNER) 71

6.2.17 Autoridad de Grupo (GRPAUT) 71

6.2.18 Autoridad (AUT) 72

Conclusiones I

Bibliografía IV

Prólogo

Prólogo

La auditoría informática representó, en su momento, una transición compleja en mi trayectoria profesional. Sin embargo, también en esta función encontré, inadvertidamente, mi verdadera vocación como apasionado de los sistemas de información computarizados. Desde su inicio, el contacto con esta actividad requirió de cambios significativos en actitud y en mi óptica de las organizaciones y sus instalaciones de cómputo. Sencillamente, no es lo mismo actuar como el "desarrollador" en plena búsqueda de la perfección algorítmica de sus aplicaciones, que fungir como el "evaluador" objetivo e independiente, capaz de identificar debilidades de control en el uso de los recursos informáticos. En este sentido, la filosofía de control requerida por el auditor también plantea la necesidad de conocer y asimilar una variedad de conceptos desconocidos y pertenecientes a otra disciplina, la Contaduría Pública. Es verdaderamente sorprendente cómo una nueva función, que en apariencia pertenece al terreno de la técnica y a la "automatización", encuentra fundamentación y se construye a partir de los cánones establecidos por una rama administrativa.

Resulta igualmente interesante y problemático el concebir a una organización como un ente socio-económico expuesto a infinidad de riesgos y amenazas, que bien podrían traducirse en pérdidas espectaculares de dinero, en la destrucción parcial o total de sus activos, en la interrupción de sus operaciones o en su irrevocable desaparición. En la generalidad de los casos, la tarea más difícil para el auditor consiste precisamente en identificar los riesgos existentes y los controles requeridos para mitigarlos. Asimismo, la explosión tecnológica ha generado nuevas exposiciones no contempladas con anterioridad y cuyas consecuencias pueden ser aún más catastróficas.

Muchos individuos coincidirían en afirmar que un centro de cómputo modelo es aquél que cuenta con una infraestructura tecnológica de hardware y software acorde con las necesidades operativas de la empresa y con un grupo de tecnócratas altamente calificados. Sin embargo, estos elementos pueden llegar a convertirse en condiciones irrelevantes, en tanto las organizaciones no procuren el establecimiento de un sistema de control interno tendiente a la salvaguarda de los activos informáticos, a elevar el nivel de integridad de los datos y a promover la efectividad y eficiencia de las aplicaciones desarrolladas.

En alguna ocasión leí que para llegar a ser un buen auditor es necesario que éste sea mejor en los negocios que sus auditados. Es justo reconocer que esta meta representa un ideal imposible de los auditores. Sin embargo, también pone de manifiesto la dificultad y el compromiso que caracterizan el quehacer cotidiano de la auditoría. La tecnología continúa evolucionando a ritmo acelerado y el reto principal del auditor consiste en mantenerse actualizado con estos nuevos avances

y en desarrollar metodologías viables para la auditoría y control de sistemas computarizados. Afortunadamente, esta evolución también ha provisto al auditor de poderosas herramientas de software que promueven una mayor eficiencia durante todo el proceso de evaluación. Estas técnicas de auditoría apoyadas en el computador seguirán perfeccionándose y predominarán en los años venideros. Sin lugar a dudas, el continuo refinamiento técnico procurado por esta novedosa y comprometedora disciplina, así como los programas de certificación establecidos por algunas asociaciones de renombrado prestigio contribuirán de manera decisiva en la formación de mejores profesionales, preparados para enfrentar y controlar la era de la tecnología de información.

Dentro de la auditoría informática existe un aspecto sobresaliente, objeto de constantes revisiones por parte de auditores internos y externos: la seguridad informática. Día con día, la importancia de esta actividad organizacional se eleva hasta niveles insospechados con la creciente dependencia de las empresas en el procesamiento electrónico de datos. Es lamentable observar, sin embargo, cómo muchos auditores concluyen equivocadamente sobre la razonabilidad de los esquemas de seguridad implantados entre sus auditados, o la negligencia de algunos altos funcionarios y empresarios, que simplemente no están dispuestos a dedicar recursos, tiempo y esfuerzo para reducir vulnerabilidades demasiado obvias. Este último hecho representa, por sí mismo, el mayor obstáculo para el responsable de planear y administrar la seguridad. Resulta imperativo, por tanto, desarrollar esfuerzos adicionales para lograr que estos personajes perciban a las tareas de protección como un costo de hacer negocio y no como un gasto innecesario, que pudiera nunca llegar a justificarse, dada la incertidumbre que rodea a la materialización de riesgos informáticos. Asimismo, es importante resaltar que la seguridad absoluta es inalcanzable y que existen amenazas que no pueden ser del todo controladas.

Muy a menudo, también es posible apreciar que algunos directores generales y gerentes de sistemas poseen ideas y puntos de vista poco realistas en torno a la seguridad. Para algunos, ésta representa una solución mágica y expedita que permite reducir riesgos a niveles aceptables. En otros casos, prevalece la creencia de que el uso de passwords y la generación de respaldos de programas, datos y documentación constituyen la única fuente posible de seguridad. En realidad, la seguridad informática siempre debe planearse cuidadosamente e incluye la implantación de un buen número de controles preventivos, detectivos y correctivos, muchos de los cuales son ejecutados por software y hardware.

Personalmente, considero que una condición suficiente y necesaria para desarrollar y concluir con éxito cualquier trabajo de auditoría es entender claramente el aspecto sujeto a revisión. Desafortunadamente, muchos auditores informáticos en nuestro país emprenden revisiones de seguridad con un conocimiento muy incipiente y superficial de la tecnología involucrada. Consecuentemente, sus conclusiones y recomendaciones resultan ser incorrectas

o también demasiado superficiales. Al parecer, el mal radica principalmente en la carencia de programas de capacitación adecuados y en la falta de fuentes bibliográficas escritas en nuesto idioma.

Dicha problemática y sus repercusiones han sido motivo de reflexiones personales importantes. El presente trabajo de investigación es una respuesta parcial a estas inquietudes y pretende apoyar al auditor informático en la comprensión de la arquitectura de seguridad del sistema IBM AS/400. He seleccionado este computador, por tratarse de una plataforma que ha logrado una difusión importante. Se estima que existen en todo el mundo al menos 250,000 equipos AS/400 en operación.

El material presentado contempla la discusión de los fundamentos de la seguridad informática y de la arquitectura operativa del AS/400, así como el análisis detallado de las características y facilidades de control de acceso lógico a objetos, provistas por el sistema operativo OS/400, en su versión 2 y release 2 (V2R2). No se ha incluido capítulo alguno con un programa de revisión de estos elementos ya que, desde mi perspectiva, esto resulta poco innovador y provechoso, a la luz de la existencia de un buen número de guías y herramientas de software en el mercado para este propósito. Además, los problemas de calidad que he observado en las evaluaciones de este tipo surgen del desconocimiento y no del método de revisión empleado.

Por último, quiero agradecer a la firma Price Waterhouse las numerosas experiencias de auditoría informática que me ha brindado. Estoy también en deuda con Claudia Sameshima por la magnífica edición de este trabajo.

Fresnillo, Zacatecas, abril de 1994.

Capítulo 1

1. Consideraciones Preliminares

Este primer capítulo es un breve análisis de los principales componentes de la seguridad informática. Se incluyen algunas consideraciones importantes sobre el resguardo y protección de los activos informáticos en una organización y la fundamentación teórica que rige la construcción de mecanismos de control de acceso lógico en computadores digitales de propósito general.

1.1 Componentes de la Seguridad Informática

El conjunto de factores que fundamentan la importancia de la seguridad informática en la actualidad incluye una lista interminable de acontecimientos, hechos y amenazas potenciales para la organización. Es justo reconocer que la ocurrencia de estas últimas no puede medirse de una manera determinística. Lo único cierto y verdadero es que el procesamiento electrónico de datos ha invadido todos los ámbitos de la actividad humana y se ha convertido en un recurso crítico e indispensable. Esto justifica plenamente la necesidad de proteger adecuadamente las instalaciones de cómputo y los activos ahí concentrados.

La seguridad informática se define como la estructura de control establecida para garantizar la integridad, confidencialidad y disponibilidad de la información almacenada electrónicamente y de los recursos de software y hardware que soportan la operación cotidiana de la organización. Esta definición establece claramente los objetivos primarios de la seguridad informática y señala también la importancia que juegan los controles en la protección de recursos.

En un sentido amplio, un control es un patrón de actividades o acciones destinadas a prevenir, detectar o corregir errores e irregularidades. Los controles de seguridad también mantienen esta orientación. Sin embargo, están diseñados para reducir el riesgo planteado por amenazas específicas, producto de fenómenos naturales y actos deliberados o accidentales de empleados o individuos ajenos a la organización. Muy a menudo, suelen apoyarse en procedimientos administrativos muy peculiares y en el uso generalizado de la tecnología. Su implantación debe ser precedida por un análisis detallado de los riesgos existentes, los costos involucrados y los beneficios a obtener.

La seguridad informática supone una problemática organizacional y, por tanto, no puede concebirse como la mera agregación de controles tecnológicos. En realidad, la integran muchos otros principios y elementos que deben considerarse minuciosamente. Todos ellos facilitan la construcción de la estructura sobre la que los controles de seguridad pueden operar eficientemente y tener éxito. Algunos de

estos componentes pretenden consolidar el apoyo y compromiso gerenciales, definir políticas y normas de seguridad adecuadas, establecer programas razonables de concientización de usuarios, etc.

El estudio de la seguridad informática comprende dos áreas principales, a saber, la seguridad física y la seguridad lógica. Las diferencias existentes entre ambas se explican en términos del tipo de recursos a proteger y la naturaleza de los controles por implantar. Esta división no revela la existencia de dos ramas mutuamente excluyentes. Los objetivos de integridad, confidencialidad y disponibilidad sólo pueden alcanzarse a través de la selección y la adopción de una combinación apropiada de controles de seguridad físicos y lógicos.

La seguridad física constituye la primera línea de defensa en la protección de los recursos informáticos. Se relaciona estrechamente con los elementos tangibles del procesamiento de datos. Estos incluyen a todas las personas, dispositivos y suministros que confluyen en un centro de cómputo. Proteger estos recursos significa controlar el acceso físico a los espacios que los albergan y mantener condiciones ambientales adecuadas en estas localidades. Existe una gran diversificación entre los controles que pueden ser utilizados para lograr estos dos objetivos. Algunos ejemplos representativos son los guardias de seguridad, todo tipo de cerraduras, el registro manual o electrónico de accesos, las identificaciones con fotografía, los sistemas biométricos de seguridad, las cámaras de video, el afianzamiento del personal de mantenimiento, los sistemas de alarma contra intrusos, los detectores de agua, los extinguidores portátiles, las alarmas de incendio manuales, los detectores de humo, los sistemas de supresión de fuego, los UPS's, los planes de contingencias y muchos más.

La seguridad lógica, por el contrario, procura controlar el acceso a recursos menos visibles, la información y los programas almacenados dentro del computador. Los controles de acceso lógico son por naturaleza preventivos ya que pretenden evitar el uso, modificación, copiado y borrado no autorizados de datos y programas. Generalmente, su implantación y ejecución se logran vía el sistema operativo y otros elementos del software de sistemas.

Las rutas de acceso del usuario desde la activación de su terminal hasta el acceso a la información pueden ser variadas e incluir varios niveles de software. A menudo, existen caminos desconocidos que pasan por alto los puntos de control establecidos en estos niveles. Este hecho descubre problemas y retos extremadamente complejos dentro del campo de la seguridad lógica.

1.2 Control de Acceso Lógico

Conceptualmente, el control de acceso lógico representa un mecanismo que permite asociar usuarios con recursos y privilegios de acción. Este vínculo siempre debe fundamentarse en la "necesidad de conocer y hacer" que presenta cada usuario del sistema. La seguridad lógica se construye, de hecho, a partir de una filosofía de acceso regida por este principio.

Bajo este modelo, las peticiones de acceso de los usuarios son procesadas en tres etapas denominadas identificación, autentificación y autorización. Debe asumirse la existencia previa de un archivo de seguridad con información sobre el usuario, los recursos y los privilegios de acción.

El usuario se identifica al proporcionar un nombre único (Figura 1). El mecanismo de control de acceso utiliza este dato como llave para localizar en el archivo de seguridad el registro que corresponde a este usuario. Si la búsqueda tienen éxito se procede a la autentificación. En caso contrario, se inicia una nueva tarea de identificación.

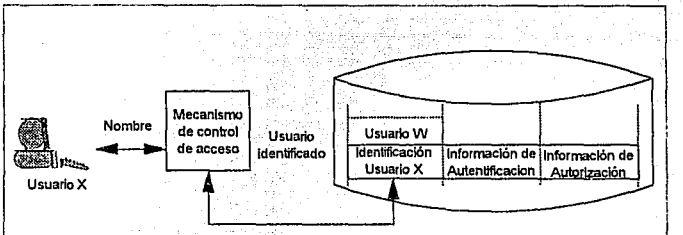


Figura 1: Identificación

Durante la autentificación, el usuario presenta una contraseña o password (Figura 2). Esta es comparada con la que se encuentra almacenada en su registro. Si el resultado muestra igualdad de contenidos se inicia la autorización. De lo contrario, se repite este ciclo.

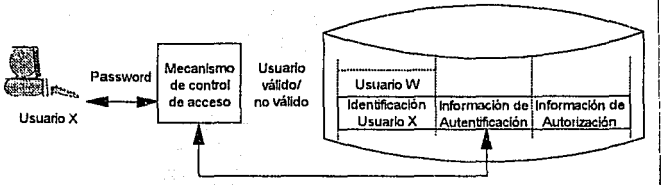


Figura 2: Autentificación

En la autorización, el usuario indica el nombre de los recursos que desea accesar y las acciones que pretende realizar con ellos (Figura 3). La suficiencia y jerarquía de los privilegios contenidos en el registro de seguridad determinan la aceptación o el rechazo de la petición usuaria.

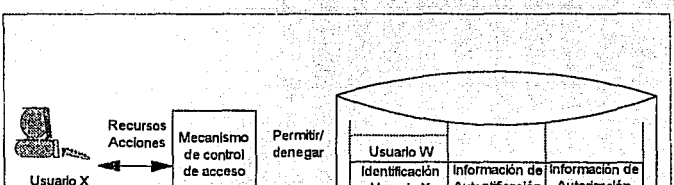


Figura 3: Autorización

La discusión anterior revela que la identificación consiste en distinguir de manera única a un usuario de los demás y que la autentificación pretende comprobar la identidad del usuario. El funcionamiento de estos dos procesos se ha explicado

con base a cierta información que el usuario proporciona al mecanismo de control de acceso. En la práctica, también pueden utilizarse objetos y características físicas (biometría) del usuario.

En el esquema propuesto, la confidencialidad de la información de autentificación suministrada por el usuario determina la capacidad de detener intentos de acceso no autorizado. Este requerimiento plantea problemas monumentales que se presentan como resultado del olvido de esta información. Muy a menudo, el usuario suple su falta de memoria con la definición de passwords que pueden ser adivinados muy fácilmente. En algunos otros casos, existe la tendencia de escribirlos en papel y de compartirlos con otras personas. Esta problemática sólo puede superarse con el establecimiento de procedimientos de administración de passwords apropiados y el establecimiento de políticas específicas.

El conjunto de privilegios de acción definidos por el mecanismo de control de acceso juega un papel preponderante en los procesos de autorización. En general, el alcance de estos privilegios debe contemplar todas las necesidades de acceso potenciales de la población usuaria. La asignación de privilegios específicos a un usuario considera únicamente sus necesidades individuales.

Finalmente, los mecanismos de control de acceso lógico pueden ser implantados en ambientes abiertos o cerrados. En un ambiente de apertura, el usuario tiene acceso a todos los recursos salvo que sus privilegios se lo impidan. Bajo una perspectiva cerrada, el usuario no puede accesar ningún recurso a menos que su registro de autorización le conceda el acceso.

Capítulo 2

2. Visión General del AS/400

Este capítulo presenta una semblanza del AS/400. Se incluyen algunos hechos que normaron en gran medida su desarrollo y construcción, así como las características fundamentales de su arquitectura. Estas últimas constituyen los elementos que permiten diferenciarlo de otros computadores y determinan, por mucho, la aceptación y difusión que ha logrado a nivel mundial.

2.1 Antecedentes

Durante la década de los 80's los usuarios de computadores propietarios IBM de alcance medio experimentan un crecimiento inusual en sus requerimientos de procesamiento. Este acontecimiento, en conjunto con los avances tecnológicos ocurridos en la industria de la computación, el agotamiento de las posibilidades de crecimiento del sistema S/36 y el éxito parcial del sistema S/38, aceleran el desarrollo del proyecto multimillonario denominado "Future System" en IBM.

Dicho proyecto concentró en Rochester, Minnesota a un gran número de profesionales, dedicados al diseño y construcción de un computador de avanzada con grandes innovaciones tecnológicas y poseedor de las siguientes características:

- Integración de las ventajas operativas de sus antecesores, los sistemas S/36 y S/38.
- Orientación hacia las necesidades de procesamiento del usuario final.
- Protección de la inversión de clientes potenciales, a través del aumento en la capacidad de crecimiento, un rendimiento superior, un solo sistema operativo para todos los modelos y una familia común de procesadores.
- Simplicidad de operación, integración de funciones avanzadas y amplia conectividad.

En junio de 1988, IBM cristaliza estos esfuerzos de ingeniería con el lanzamiento al mercado de los nueve modelos de la serie B del Application System/400 (AS/400). Desde entonces, prácticamente toda la base instalada de equipos S/36 y S/38 en el mundo se ha visto disminuida en favor del AS/400. Cabe también resaltar que durante el primer año de su fabricación se vendieron alrededor de 30,000 unidades. Esta cifra representa un hecho sin precedentes en la industria.

En la actualidad, la familia de sistemas AS/400 consta de catorce modelos distintos de procesadores centrales, pertenecientes a la serie F. Todos éstos se agrupan bajo las presentaciones 9402, 9404 y 9406, de la siguiente manera:

- 9402 - Modelos F02, F04 y F06
- 9404 - Modelos F10, F20 y F25
- 9406 - Modelos F35, F45, F50, F60, F70, F80, F90 y F95

Los seis procesadores 9402 y 9404 son los más pequeños y están diseñados para operar bajo condiciones ambientales típicas de oficina. Muy a menudo, se encuentran ubicados debajo de escritorios o en las esquinas de áreas y espacios físicos de trabajo. Por lo que se refiere a los procesadores 9406, se encuentran empotrados en gabinetes o racks más grandes. Esta característica facilita la expansión y crecimiento en hardware. Generalmente, se localizan en áreas independientes al resto de la organización, debidamente acondicionadas. La Figura 4 muestra la apariencia de los gabinetes de los procesadores 9402, 9404 y 9406.

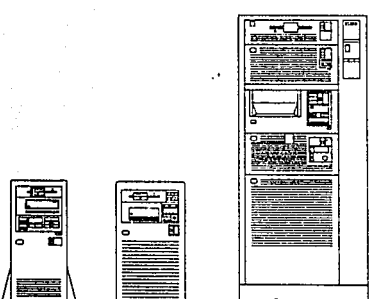


Figura 4: Presentaciones del AS/400

Las Tablas 1-3 describen las principales diferencias entre todos los modelos de la serie F.

	Modelo 9402		
	F02	F04	F06
Memoria (MB)	8-24	8-24	8-40
DASD (MB) Mínimo Máximo	 988 1,976	 988 3,952	 988 7,904
Número máximo de estaciones de trabajo tipo 5250 ASCII	 28 18	 68 66	 108 102
Líneas de comunicaciones	0-8	1-8	1-14
Adaptadores LAN	0-1	0-1	0-2
Rendimiento relativo	1.9	2.5	3.3
Número de buses de I/O	1	1	2

Tabla 1: Resúmen de las Capacidades de los Modelos 9402 F02, F04 y F06

	Modelo 9404		
	F10	F20	F25
Memoria (MB)	8-72	16-80	16-80
DASD (MB) Mínimo Máximo	 988 11,850	 988 11,850	 988 15,800
Número máximo de estaciones de trabajo tipo 5250 ASCII	 160 162	 240 162	 240 162
Líneas de comunicaciones	1-14	1-20	1-26
Adaptadores LAN	0-2	0-4	0-4
Rendimiento relativo	3.4	4.2	4.8
Número de buses de I/O	2	2	2

Tabla 2: Resúmen de las Capacidades de los Modelos 9404 F10, F20 y F25

	Modelo 9406							
	F35	F45	F50	F60	F70	F80	F90	F95
Memoria (MB)	16-80	16-80	64 - 192	128-384	128-512	128-512	128-512	128-512
DASD (MB)								
Mínimo	1,970	1,970	1,970	1,970	1,970	1,970	1,970	1,970
Máximo	39,300	39,300	74,700	110,100	165,200	165,200	165,200	165,200
Número máximo de estaciones de trabajo								
tipo 5250	480	720	1000	1400	2400	2400	2400	2400
ASCII	216	324	450	630	1080	1080	1080	1080
Líneas de comunicaciones	1-20	1-33	1-33	1-49	1-64	1-64	1-64	1-64
Adaptadores LAN	0-4	0-4	0-4	0-4	0-6	0-6	0-6	0-6
Rendimiento relativo	48	60	102	147	210	365	471	547
Número de buses de I/O	2	2	3-5	3-5	3-7	3-7	3-7	3-7

Tabla 3: Resúmen de las Capacidades de los Modelos 9406 F35, F45, F50, F60, F70, F80, F90 y F95

La Figura 5 es una comparación gráfica del rendimiento relativo de estos equipos. Debe asumirse un valor de 1 para el modelo B10, un porcentaje de utilización del 70% y configuraciones máximas en todos los modelos.

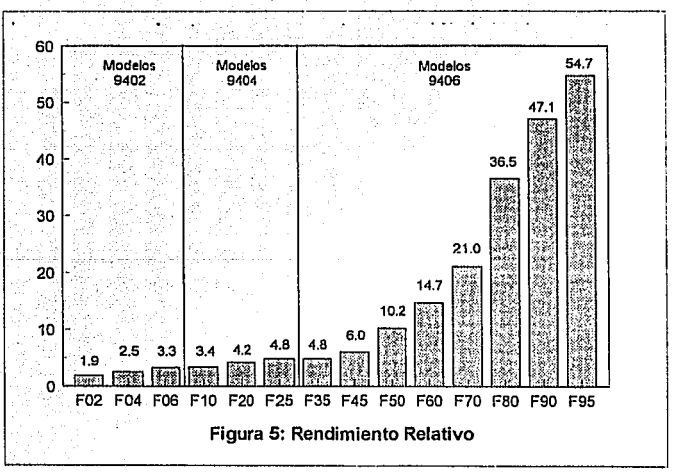


Figura 5: Rendimiento Relativo

Muchos especialistas y críticos han coincidido en afirmar que una de las fortalezas del AS/400 sobre otros computadores es la extensa variedad de productos de software disponible. La lista inicia con un sistema operativo único para todos los procesadores, el OS/400, e incluye también programas de soporte general al sistema, compiladores y herramientas para el desarrollo de aplicaciones, programas de comunicaciones y conectividad, aplicaciones multimedia, soluciones integrales para los negocios y muchos más.

2.2 Arquitectura

El sistema AS/400 ha sido diseñado como un sistema total. Esto significa que muchas de las funciones realizadas tradicionalmente por software de aplicación han sido integradas en el sistema operativo y en la máquina. El usuario se comunica con todas estas funciones a través de un solo lenguaje de control o con el uso de los menús y peticiones del sistema.

El AS/400 es un computador de propósito general para los negocios. Su diseño refleja las exigencias predominantes de estos entornos:

- Facilidad de uso, desde la perspectiva del operador y el usuario final.
- Habilidad para crecer y absorber avances tecnológicos, sin provocar interrupciones.
- Optimización para trabajos intensivos de entrada/salida (I/O).

La arquitectura del AS/400 incluye cinco características distintivas que permiten diferenciarlo de otros equipos existentes en el mercado. Las siguientes secciones explican estos atributos.

2.2.1 Máquina de Alto Nivel

El AS/400 aisla a los usuarios de las características propias del hardware a través de una arquitectura estratificada. Este concepto permite elevar el nivel de la interfase de máquina y crear un conjunto de instrucciones de máquina de alto nivel, que es independiente de la implantación específica de hardware.

La Figura 6 muestra el hardware y el código interno bajo licencia que componen la máquina de alto nivel. El AS/400 es muy peculiar en cuanto a que la máquina se define por software y no por hardware. Las instrucciones presentadas a la interfase de máquina son objeto de un proceso adicional de traducción antes de ser entendidas por el hardware. El código interno bajo licencia es el responsable de ejecutar este proceso. Las características del hardware se ven modificadas con los avances tecnológicos; sin embargo, el usuario sigue observando la misma interfase de máquina gracias a este código interno.

Adicionalmente, algunas rutinas residentes en el sistema operativo de una máquina convencional han sido transladadas al código interno bajo licencia del AS/400. Este hecho genera ventajas importantes en rendimiento y velocidad de ejecución.

La arquitectura estratificada significa que las nuevas tecnologías de hardware y software pueden ser incorporadas, sin afectar las aplicaciones existentes.

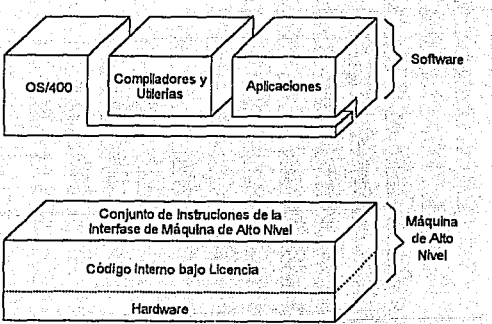


Figura 6: Máquina de Alto Nivel

2.2.2 Orientación hacia Objetos

Todo lo que puede ser almacenado y recuperado en el AS/400 se encuentra contenido en un "objeto". Los objetos logran independizar a los usuarios de las técnicas específicas de implantación utilizadas en la máquina. Siempre cuentan con un nombre y un tipo. Su estructura incluye un encabezado común y una porción funcional que depende del tipo. Esta característica permite combinar en una sola entidad datos y métodos válidos para utilizar éstos.

La existencia de objetos mejora los niveles de integridad del sistema y sus datos, ya que es posible llevar a cabo funciones estándar a nivel de todos los objetos y limitar el conjunto de operaciones que pueden realizarse sobre objetos específicos. Asimismo, el usuario no requiere considerar el espacio ocupado por sus objetos; el sistema lo asigna automáticamente.

2.2.3 Almacenamiento de un Solo Nivel

Todo el almacenamiento en el sistema, sea memoria principal o espacio de acceso directo en disco, es direccionado de la misma manera. Este mecanismo es único e independiente de cualquier dispositivo y permite accesar un objeto a través de su nombre. Todos los objetos son tratados como si residieran en un espacio de direccionamiento de 281,000,000,000,000 bytes.

El direccionamiento virtual del AS/400 es independiente de la ubicación física del objeto y del tipo, capacidad y número de unidades de disco instaladas en el sistema.

Los programas de aplicación no requieren ser modificados para integrar nuevas tecnologías de almacenamiento y los usuarios delegan a la máquina la administración total del almacenamiento.

La Figura 7 es una representación pictórica de este esquema virtual de almacenamiento.

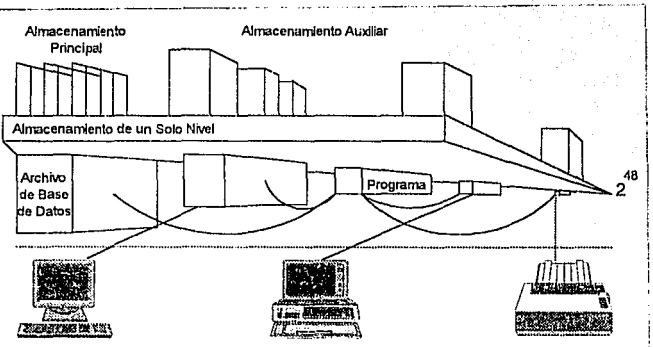


Figura 7: Almacenamiento de un Solo Nivel

2.2.4 Jerarquía de Microprocesadores

La Figura 8 muestra la existencia de procesadores adicionales en el AS/400, cada uno dedicado a un tipo particular de dispositivo de entrada/salida. Esta característica permite que el procesador principal pueda delegar al microprocesador pertinente todo tipo de solicitudes de escritura o de lectura de datos en un dispositivo y continuar con la ejecución de otro programa de aplicación. En un modelo 9406 F95 totalmente configurado pueden encontrarse alrededor de doscientos procesadores.

Este diseño otorga al AS/400 un rendimiento superior en los ambientes comerciales basados en el procesamiento intensivo de transacciones. Asimismo, las últimas tecnologías de microprocesadores pueden ser incorporadas en cualquier momento sin ocasionar interrupciones en el resto del sistema.

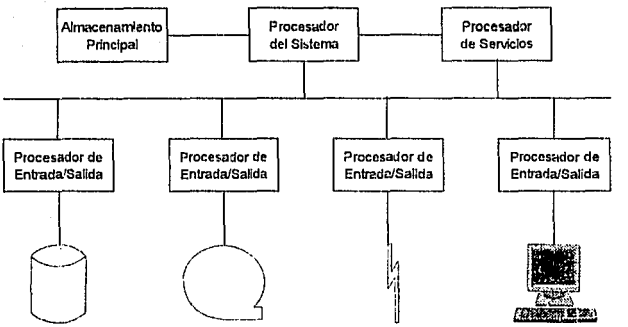


Figura 8: Jerarquía de Procesadores

2.2.5 OS/400

La Figura 9 describe el enfoque tradicional utilizado para el diseño de sistemas operativos. Bajo este esquema, el sistema operativo requiere de la adición de múltiples componentes de software con facilidades de administración de la base de datos, soporte de comunicaciones, procesamiento interactivo, implantación de mecanismos de seguridad, etc. Frecuentemente, estos productos son desarrollados por terceras partes. Su incorporación al sistema operativo debe, por tanto, estudiarse detenidamente para evitar problemas de compatibilidad.

En el AS/400, estos aspectos no son relevantes, ya que el OS/400 ha integrado estos componentes en su totalidad. OS/400 contiene software para el soporte de todos los servicios descritos y mucho más. Asimismo, puede operar simultáneamente en varios idiomas.

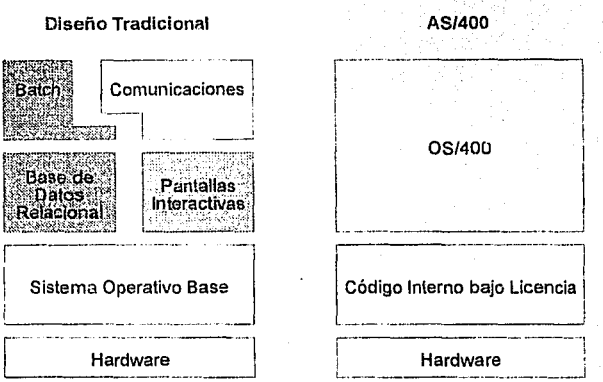


Figura 9: Sistemas Operativos

Capítulo 3

3. Terminología Básica del AS/400

Este capítulo es una introducción a la terminología básica del AS/400. Muchas de las definiciones aquí presentadas pueden resultar triviales; sin embargo, deben ser comprendidas claramente antes de explorar las características de seguridad de este sistema. Mucha de esta jerga técnica proviene del IBM S/38 y tiene, en la generalidad de los casos, el mismo significado.

3.1 Lenguaje de Control

OS/400, el sistema operativo del AS/400, mantiene como interfase primaria del usuario el lenguaje de control denominado Control Language (CL). Este representa una colección muy grande de comandos, que permite a usuarios interactivos y programas de aplicación un acceso consistente a todas las funciones del sistema. Los comandos de CL pueden agruparse y compilarse para ejecutar funciones operativas complejas. Estos programas pueden invocar a o ser llamados desde cualquier otro programa escrito en lenguaje de alto nivel. También pueden accesar la base de datos relacional integrada en el sistema y comunicarse directamente con el usuario, a través de desplegados y peticiones. CL es, de hecho, una interfase de alto nivel extendible, con una sintáxis coherente para desarrollar funciones operativas, de programación y de mantenimiento.

3.2 Objetos

Prácticamente todo aquello que puede ser almacenado o recuperado en el AS/400 recibe el nombre de objeto. Un objeto contiene datos estructurados y un conjunto de instrucciones y reglas para uso de éstos. Los programas, archivos, perfiles de usuario, bibliotecas, colas de trabajo, colas de salida, comandos, documentos y descripciones de dispositivos son objetos. El mecanismo de seguridad del sistema controla el acceso a nivel de objeto. Todo objeto también cuenta con un propietario, concepto que juega un papel importante en las funciones de seguridad. Por ejemplo, un perfil de usuario no puede ser eliminado a menos que todos los objetos de los que es propietario sean borrados o asignados a otro perfil. Existe un comando disponible para cambiar la propiedad sobre objetos (CHGOBJOWN), que requiere de autoridad apropiada para ser utilizado.

Los registros en un archivo o los campos de un registro no se consideran objetos. Por tanto, el acceso no se controla directamente a este nivel.

Todos los objetos se describen a través de un nombre y un tipo. Existen más de 40 tipos de objetos diferentes. En particular, los tipos *FILE (archivo), *USRPRF (perfil de usuario), *PGM (programa) y *LIB (biblioteca) son importantes desde una perspectiva de seguridad.

Existe, además, un encabezado invisible (header) de 512 bytes en cada objeto. Dicho header siempre contiene un apuntador hacia el perfil de usuario propietario del objeto, la autoridad pública (*PUBLIC) del objeto y, en algunos otros casos, un apuntador a una lista de autorización opcional. Los headers son una parte integral de cualquier objeto.

Ocasionalmente, las definiciones de tipo pueden manejarse a dos niveles con el concepto de atributo (subtipo). Algunos atributos del tipo *FILE son:

- DDMF Archivo de dispositivo para accesar un sistema remoto
- DKTF Archivo de dispositivo para un disco flexible
- DSPF Archivo de dispositivo para un desplegado
- ICFF Archivo de dispositivo para una línea de comunicaciones
- PF Archivo físico
- LF Archivo lógico
- PRTF Archivo de impresión
- SAVF Archivo de salvado y recuperación de datos
- TAPF Archivo de dispositivo para cinta magnética

La mayoría de los objetos residen en bibliotecas (también objetos), algunas creadas por usuarios y otras provistas implícitamente por el sistema. El nombre de los objetos tiene una longitud máxima de 10 caracteres. Las bibliotecas tienen un nombre único. El nombre de cualquier otro tipo de objeto consiste de dos partes: el nombre intrínseco del objeto (10 caracteres) y un calificador en la forma del nombre de la biblioteca (otros 10 caracteres) del objeto. El tipo del objeto constituye otra distinción menos visible.

Los nombres de las bibliotecas deben ser únicos dentro del sistema. Los nombres de objetos también deben ser únicos dentro de su biblioteca y tipo. En general, el nombre de los objetos requeridos o creados por el AS/400 para su operación inicia con la letra Q. Los usuarios no deben, por tal motivo, utilizar nombres para sus objetos que comiencen con esta letra. El nombre del objeto en los siguientes ejemplos es siempre OBJ1. Sin embargo, los nombres de bibliotecas y tipos utilizados identifican de manera única a este objeto.

- PW/OBJ1 *FILE archivo OBJ1 en biblioteca PW
- PW/OBJ1 *PGM programa OBJ1 en biblioteca PW
- PW/OBJ1 *MENU menú OBJ1 en biblioteca PW
- CL/OBJ1 *FILE archivo OBJ1 en biblioteca CL

Estos cuatro objetos pueden existir simultáneamente sin conflictos de nombramiento.

Resulta importante, desde un punto de vista de seguridad y de administración del sistema, que la mayoría de los nombres de objetos logren autoidentificarse y adopten estrictamente nomenclaturas bien definidas.

3.3 Asignación y Direccionamiento de Espacio de Almacenamiento

La asignación de espacio de almacenamiento en el AS/400 es muy diferente a la de casi todos los computadores grandes de IBM. El AS/400, como el S/38, cuenta con un rango de direccionamiento de 48 bits. Todo este rango constituye un espacio único de direccionamiento virtual. Cualquier objeto se encuentra en memoria virtual. El almacenamiento en disco es meramente almacenamiento de paginación para esta memoria virtual. Un usuario normal no puede accesar la totalidad de esta memoria; sólo puede direccionar las partes (objetos) para las que cuenta con autorización. Los nombres internos de los objetos son realmente las direcciones virtuales ocupadas por éstos en este sistema de almacenamiento de nivel único.

3.4 Bibliotecas

Cuando se crea un objeto, éste debe encontrarse en una biblioteca. Si se desea accesar un objeto, debe conocerse el nombre de la biblioteca pertinente. En los casos en que este nombre no sea especificado, el sistema utiliza la llamada lista de bibliotecas para localizar el objeto.

La lista de bibliotecas (*LIBL) representa el ambiente de bibliotecas en el que cualquier trabajo (job) del usuario es ejecutado. La biblioteca actual es la biblioteca primaria con la que el usuario trabaja; todo objeto de nueva creación es depositado en ella. La lista de bibliotecas contiene los nombres de todas las bibliotecas a utilizar en la búsqueda de objetos e incluye a la biblioteca actual.

Una biblioteca es un tipo de objeto cuya única función es la de agrupar objetos. No agrupa otras bibliotecas y no contiene objetos, ya que sólo es un directorio.[1]

Ciertas bibliotecas son provistas por el propio AS/400 y representan partes integrales de todo el sistema. Otras son creadas por los usuarios y algunas más están incluídas en los productos de software desarrollados por terceras partes. Entre las pertenecientes al sistema destacan QSYS, QGPL, QTEMP, QSPL, QGDDM, QSRV, QRCL y QRECOVERY. Los usuarios deben evitar añadir objetos a estas bibliotecas de IBM.

Las reglas de acceso a bibliotecas gobiernan el uso de comandos, programas y archivos. Se debe tener necesariamente acceso a la biblioteca y al objeto que desea utilizarse. El sistema localiza el programa o comando en las bibliotecas especificadas en *LIBL o también puede señalarse explícitamente su ubicación al intentar ejecutarlos.

El comando DSPLIBL es comúnmente utilizado para desplegar el contenido de la lista de bibliotecas asignada al trabajo de un usuario.

3.5 Archivos

Existen cuatro categorías generales de archivos presentes en el AS/400:

- Archivos de Datos

  Contienen generalmente transacciones, datos de archivos maestros o programas fuente.

---

[1] La única excepción es la biblioteca del sistema denominada QSYS, que puede agrupar objetos y otras bibliotecas.

- Archivos de Dispositivos

  Incluyen referencias a medios externos, tales como cintas, diskettes, terminales, impresoras u otros sistemas conectados a través de líneas de comunicaciones.

- Archivos de Gestión Distribuída de Datos

  Contienen la información de ruteo requerida para accesar archivos almacenados en otro sistema.

- Archivos de Salvado

  Utilizados para la generación de respaldos en línea y para la transferencia de datos a otros sistemas AS/400.

Un archivo puede contar con miembros, que usualmente incluyen datos o descripciones de datos. En el caso de archivos de datos se presenta frecuentemente un solo miembro con muchos registros. Por el contrario, los archivos con código fuente pueden agrupar varios miembros, uno por cada programa fuente.

Los comandos y los programas ejecutables residen en bibliotecas a nivel de objetos; no pueden constituir miembros de un archivo.

Las autoridades (permisos de acceso) de un archivo aplican por igual a todos sus miembros. Existen también autoridades individuales para cada miembro. Sin embargo, éstas no tienen ningún efecto o visiblidad al usuario normal, ya que no se cuenta con comandos para manipularlas.

3.5.1 Archivos Físicos

Los archivos físicos de datos contienen dos partes: una sección con la descripción de los campos en el archivo y otra sección con los datos. La descripción del registro se mantiene en una porción del objeto separada de los datos. Es necesario crear primero la descripción para estar en posibilidad de escribir registros en el archivo.

3.5.2 Archivos Lógicos

Un archivo lógico es la descripción de elementos provenientes de uno o más archivos físicos. Estos elementos incluyen los campos a utilizar, el orden de clasificación y el criterio de selección de registros. Este tipo de archivos representan, de hecho, una manera de mapear campos y/o registros específicos de archivos físicos. Los campos y registros no seleccionados no están disponibles para su procesamiento. Esta característica permite el diseño de métodos de control de acceso a los datos contenidos en archivos físicos.

En general, los archivos lógicos se usan de la misma manera que los archivos físicos. Es justo reconocer que ofrecen algunas facilidades adicionales, como las opciones booleanas de filtración de campos y registros al momento de su creación.

La Figura 10 muestra las principales diferencias conceptuales entre los archivos físicos y lógicos.

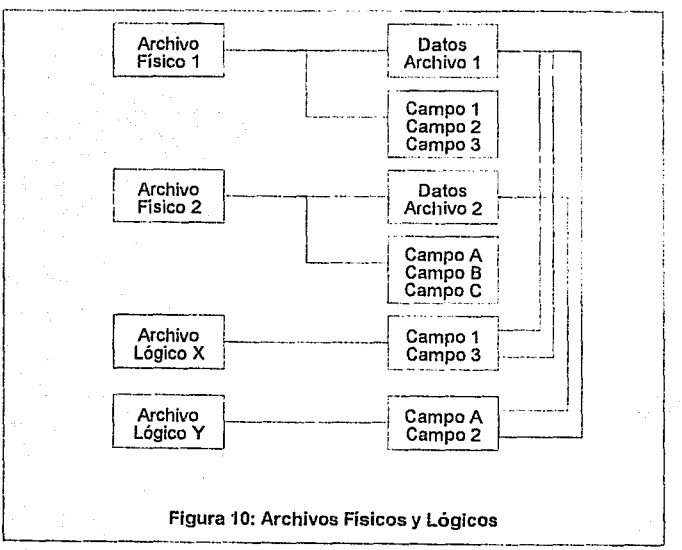


Figura 10: Archivos Físicos y Lógicos

3.6 Diccionarios de Datos

Se puede crear un diccionario de datos para todos los archivos en una biblioteca. Esta herramienta permite establecer definiciones de campos y formatos que pueden ser utilizados por múltiples programas. Este hecho facilita grandemente la generación de programas para accesar cualquier archivo disponible en la biblioteca. Todos los nombres de campos de los diferentes registros en los archivos pueden localizarse con el uso del diccionario.

El diccionario siempre tiene el mismo nombre de la biblioteca que representa y sólo puede ser creado para objetos de tipo *FILE.

3.7 Trabajos

El término trabajo (job) en el AS/400 se refiere a cualquier proceso interactivo, por lotes (batch) o del sistema, que es iniciado y ejecutado. Asociado a un trabajo siempre existe una descripción (job description) que contiene un conjunto específico de atributos, tales como cola de trabajo a utilizar, prioridad de ejecución, severidad de la cola de mensajes asignada al trabajo, datos de ruteo, lista de bibliotecas e información de salida. Estos atributos determinan la manera en que el trabajo corre en el sistema. Existen cinco tipos de trabajos con relevancia para la seguridad:

- Trabajos interactivos iniciados por los usuarios al firmarse al sistema.
- Trabajos en lotes iniciados por los usuarios desde sus terminales.
- Trabajos en lotes iniciados por los operadores del sistema.
- Trabajos de comunicaciones con otros sistemas.
- Trabajos de autoarranque del propio sistema para ejecutar tareas rutinarias.

3.8 Colas de Trabajo

Una cola de trabajo (job queue o JOBQ) es una lista de trabajos batch en espera de ser ejecutados por el sistema. Se encuentra asociada a un ambiente de procesamiento denominado subsistema y también a una descripción llamada JOBQD. Un trabajo es colocado en la cola de trabajo con el comando SBMJOB.

Los trabajos son seleccionados para su ejecución en el subsistema de acuerdo a su prioridad. Es posible incluir información de seguridad en JOBQD para controlar el acceso a la cola de trabajo y a los trabajos ahí residentes.

3.9 Subsistemas

Un subsistema es un ambiente operativo predefinido y único, utilizado por el AS/400 para coordinar el flujo de trabajo y el uso de recursos. Representa un vehículo separador de las actividades en el sistema. Cada tarea realizada en el susbsistema es un trabajo. Contiene, además, registros que permiten identificar las fuentes desde las que los trabajos pueden ser iniciados y ejecutados. Es posible definir varios subsistemas en un equipo AS/400.

Existen varias configuraciones estándar de subsistemas, algunas provistas por IBM y otras inmersas en productos de software licenciados. En la práctica, suele optarse por una combinación de configuraciones para separar la carga de trabajo en el sistema. Estas mezclas pueden incluir subsistemas definidos por IBM, algunos paquetes de software o el propio usuario.

Algunos de los subsistemas proporcionados por IBM son QBASE, QCMN, QCTL, QINTER, QPGMR, QSNADS, QSPL, QSYSSBSD, QDSNX, QFNC y QTCP.

3.10 Descripciones de Configuración

Las descripciones de configuración se utilizan para definir las características y el arreglo de los dispositivos y enlaces de comunicación conectados al AS/400. Sobresalen las siguientes descripciones:

- Líneas (LIND)
- Controladores (CTLD)
- Dispositivos (DEVD)
  - Impresoras
  - Terminales
  - Unidades de cinta y diskette
  - Dispositivos de comunicaciones

- Modos (MODD)
- Clases de servicio (COS)

El AS/400 posee la capacidad de crear automáticamente ciertas descripciones de configuración para controladores y dispositivos locales. Esta característica reduce significativamente las tareas de instalación y puesta en marcha iniciales del sistema.

3.11 Colas de Salida

Una cola de salida (output queue o OUTQ) es una lista de archivos en espera de ser impresos. Son objetos utilizados para definir los atributos de las salidas de los trabajos en el sistema. El subsistema en el que corre un trabajo genera y coloca los archivos de salida en la cola de salida asignada a este trabajo.

3.12 Salidas del Sistema

Las salidas del sistema (system exits) son interrupciones en el flujo normal de control del sistema operativo, que permiten la inserción de código adicional para la sintonización de muchas de las funciones de supervisión y monitoreo normalmente ejecutadas. Las características operativas de un sistema pueden verse modificadas sustancialmente con el uso generalizado de estas interrupciones.

El AS/400 cuenta con cuatro salidas del sistema disponibles. Su uso supone la especificación de programas en ciertos valores del sistema y atributos de red. El programa es invocado cada vez que el valor o atributo es revisado por el sistema operativo. Las cuatro salidas del sistema se muestran a continuación:

- QRMTSIGN

  Valor del sistema utilizado para administrar el acceso de usuarios desde sistemas remotos.

- QPWDVLDPGM

  Valor del sistema usado para validar contraseñas (passwords).

- DDMACC

  Atributo de red para controlar accesos de funciones DDM

- PCSACC

  Atributo de red que controla el acceso de usuarios vía la herramienta PC Support.

3.13 Programas y Comandos

La terminología del AS/400 distingue programas y comandos. Un comando se utiliza para demandar una función del sistema. Consiste de un nombre y parámetros opcionales, que definen mayor detalle sobre el comando. Los usuarios pueden crear sus propios comandos a través del uso del comando CRTCMD. Todo comando invoca código del programa procesador de comandos (Command Processing Program o CPP).

Un programa se refiere a código fuente preparado por el usuario o un fabricante de software, escrito en un lenguaje como CL, RPG, Cobol, etc. Existen en la forma de miembros de archivos, que son compilados para crear un nuevo objeto de tipo *PGM. Los programas pueden invocarse desde una terminal con el comando CALL.

Los comandos y los programas están sujetos a todos los esquemas de protección y seguridad que ofrece el AS/400, en virtud de que también son objetos.

Capítulo 4

4. Características de Seguridad del AS/400

Las secciones de este capítulo analizan las principales características de seguridad del AS/400. Algunos de los conceptos y tópicos explicados serán tratados con mayor profundidad en los próximos capítulos.

4.1 Perfiles de Usuario

Los perfiles de usuario constituyen el núcleo principal de la seguridad y el control de acceso en los sistemas AS/400. Son objetos especiales que describen a un usuario del sistema y definen sus privilegios y limitaciones con respecto al uso de los recursos almacenados. Contienen apuntadores hacia los objetos propiedad del usuario y también hacia los que puede acceder. Adicionalmente, cuentan con listas de usuarios que pueden utilizar los objetos de los que el usuario es propietario.

Todo perfil cuenta con un nombre, conocido como "identificador del usuario" o user-id. Esta es la clave que, junto con la contraseña, el usuario proporciona durante la sesión inicial de conexión al sistema (sign-on o firma) desde su terminal de trabajo.

4.2 Autoridades Especiales

Todos los sistemas de seguridad cuentan con privilegios especiales para desarrollar ciertas tareas de seguridad y administración. El AS/400 no es la excepción y define los siguientes seis privilegios, denominados autoridades especiales:

- *ALLOBJ - All Object

  Representa el privilegio de usuario más alto, ya que otorga derechos ilimitados para definir, modificar, borrar y accesar cualquier recurso del sistema. El poder de *ALLOBJ no incluye, sin embargo, la creación y mantenimiento de perfiles de usuario. Resulta evidente que *ALLOBJ debe asignarse de una manera extremadamente restrictiva.

- *SECADM - Security Administrator

  Permite al usuario desarrollar funciones de adición de usuarios, cambio y desplegado de autoridades sobre objetos, adición y remoción de códigos de acceso, etc. En general, *SECADM se requiere para administrar perfiles de usuario.

- *SAVSYS - Save System

  Otorga al usuario la facilidad de utilizar las funciones de salvado y recuperación de todos los objetos en el sistema.

- *JOBCTL - Job Control

  Proporciona capacidades típicas de un operador, tales como manipulación de colas de trabajo y de salida, control general sobre trabajos, subsistemas e inicialización del sistema (IPL).

- *SERVICE

  Generalmente utilizada por ingenieros de servicio de IBM o programadores de sistemas para desarrollar funciones de mantenimiento al sistema operativo y algunas otras tareas especializadas.

- *SPLCTL - Spool Control

  Otorga control absoluto sobre los archivos de impresión en colas de salida.

4.3 Clases de Usuario

Existen cinco clases de usuario jerárquicas (*USRCLS) que representan distintos roles en un ambiente de procesamiento de datos. Dentro de esta jerarquía, una clase alta está en posibilidad de desarrollar todas las funciones de una clase más baja. Las clases disponibles son:

- *SECOFR Oficial de Seguridad
- *SECADM Administrador de la Seguridad
- *PGMR Programador
- *SYSOPR Operador del Sistema
- *USER Usuario Final

Las autoridades especiales descritas anteriormente pueden ser asignadas automáticamente por el sistema, de acuerdo a la clase seleccionada para el usuario. Las Tablas 4 y 5 muestran la relación de clases y autoridades especiales. En este sentido, resulta importante señalar que las asociaciones posibles dependen del nivel de seguridad en el que opera el sistema. Este concepto será analizado posteriormente.

	Autoridades Especiales					
Clase	*ALLOBJ	*SECADM	*SAVSYS	*JOBCTL	*SERVICE	*SPLCTL
*SECOFR	X	X	X	X	X	X
*SECADM	X	X	X	X		
*PGMR	X		X	X		
*SYSOPR	X		X	X		
*USER	X		X			

Tabla 4: Correspondencia entre clase y autoridades especiales bajo los niveles de seguridad 10 y 20

	Autoridades Especiales					
Clase	*ALLOBJ	*SECADM	*SAVSYS	*JOBCTL	*SERVICE	*SPLCTL
*SECOFR	X	X	X	X	X	X
*SECADM		X	X	X		
*PGMR			X	X		
*SYSOPR			X	X		
*USER						

Tabla 5: Correspondencia entre clase y autoridades especiales bajo los niveles de seguridad 30 y 40

El oficial de seguridad o el administrador de la seguridad pueden asignar explícitamente las autoridades especiales, cuando una de las clases estándar no contemple la combinación apropiada de autoridades.

La clase de usuario también determina las opciones que son mostradas en los menús del sistema operativo. Un usuario con mayores autoridades tendrá acceso a un mayor número de elementos, mientras que un usuario de bajo nivel no visualizará las opciones que no puede usar.

4.4 Perfiles de IBM

El AS/400 posee varios perfiles de usuario como parte del sistema operativo. Algunos de éstos se utilizan para lograr acceso al sistema. Otros fueron creados como propietarios de ciertos objetos especiales. Sobresalen los siguientes:

QSECOFR	QPGMR	QUSER
QSYSOPR	QSRVBAS	QSRV
QSPL	QSYS	QSPLJOB
QRJE	QDOC	QSNADS
QFNC	QDBSHR	QTSTRQS
QGATE	QDFTOWN	QDSNX

4.5 Perfiles de Grupo

Un perfil de usuario puede ligarse a un perfil de grupo, concepto heredado del S/38. Esto permite que todos los miembros de un grupo compartan atributos, acceso a archivos y propiedad sobre objetos. Un usuario puede pertenecer a un solo perfil de grupo y únicamente se permite un nivel de agrupamiento. Por ejemplo, si el usuario CARLOS pertenece al grupo DEPTO1 (que es también un perfil), DEPTO1 no puede ligarse a otro perfil grupal.

Los perfiles de grupo se usan para organizar usuarios de acuerdo a las funciones desempeñadas y para simplificar la asignación y administración de autoridades sobre objetos. El diseño de grupos requiere necesariamente de la comprensión de los conceptos de propiedad grupal y del uso de reglas de nombramiento.

Un perfil de grupo se implementa como un perfil de usuario convencional. El AS/400 reconoce un perfil de grupo al adicionar su primer miembro. Sin embargo, es recomendable mantener a estos perfiles especiales como entidades separadas. Un apoyo en esta dirección es evitar las firmas de usuarios (sign-on's) a los perfiles de grupo.

4.6 Capacidades Limitadas

A un usuario se le pueden asignar capacidades limitadas (LMTCPB) durante la creación de su perfil. Esta característica, en conjunto con el uso de un programa inicial (INLPGM) o un menú inicial (INLMNU), puede limitar al usuario a un subconjunto específico de funciones del sistema.

LMTCPB puede ser parcial o completa. Las funciones afectadas son el programa inicial, el menú inicial, la biblioteca actual, el programa de atención actual (asociado con la tecla de atención en la terminal) y el acceso a comandos generales del sistema. La palabra clave ALWLMTUSR en los comandos puede utilizarse (con autoridad apropiada) para permitir a usuarios con LMTCPB acceso a comandos adicionales.

4.7 Autoridades Específicas

El sistema de seguridad del AS/400 está orientado primordialmente a la protección de objetos, en virtud de que todas las estructuras de datos almacenadas, tanto de usuarios como del sistema, son objetos. Todos los objetos tienen estructuras comunes en sus bloques de control (invisibles al usuario normal). Esto permite un enfoque unificado de seguridad, ya que los objetos interactúan de la misma manera con las rutinas de seguridad.

En terminología AS/400, una autoridad es el permiso requerido para accesar un objeto. El propietario del objeto y el oficial de seguridad (u otro usuario con *ALLOBJ) pueden otorgar y revocar la autoridad a un objeto con el uso de los comandos GRTOBJAUT y RVKOBJAUT. Existe una variedad de términos y conceptos que usan la palabra autoridad. Es importante entender la diferencia entre la autoridad a un objeto y la autoridad a los datos de un objeto. Algunas operaciones como crear, mover, renombrar, salvar o borrar aplican al objeto como tal. Es posible contar con autoridad para estas operaciones sin tener acceso a los datos almacenados en el objeto. De la misma manera, se puede mantener acceso total a los datos de un objeto (leer, escribir, actualizar o borrar), sin poseer autoridad para manipular el objeto.

Las siguientes autoridades son independientes, no jerárquicas. Para algunas operaciones se requiere una combinación de autoridades.

- *OBJOPR - Object Operational

  Controla el uso de un objeto y la capacidad de visualizar su descripción. Se requiere para abrir un archivo y, por tanto, se utiliza en combinación con otros derechos sobre los datos.

- *OBJMGT - Object Management

  Controla el movimiento y el renombramiento de objetos, las funciones de cambio de atributos de un objeto y las funciones de otorgamiento y revocación de autoridades a otros usuarios o grupos.

- *OBJEXIST - Object Existence

  Controla las operaciones de borrado, salvado, recuperación o de transferencia de propiedad de objetos.

- *AUTLMGT - Authorization List Management

  Se requiere para manipular el contenido de una lista de autorización. Es un permiso especializado que generalmente no es agrupado con las otras autoridades especificas.

- *READ

  Controla la habilidad de leer y recuperar los datos de un objeto.

- *ADD

  Controla la habilidad de insertar nuevos datos (entradas) en un objeto.

- *UPDATE o *UPD

  Controla la habilidad de modificar entradas existentes en un objeto.

- *DELETE o *DLT

  Controla la habilidad de borrar entradas existentes en un objeto.

Existen también algunas combinaciones de estas autoridades denominadas *ALL, *CHANGE, *USE y *EXCLUDE. La Tabla 6 muestra las equivalencias definidas. La autoridad *AUTLMGT es un caso especial y, por tanto, no se incluye.

	Autoridades Específicas						
Combinación	*OBJOPR	*OBJMGT	*OBJEXIST	*READ	*ADD	*UPD	*DLT
*ALL	X	X	X	X	X	X	X
*CHANGE	X			X	X	X	X
*USE	X			X			
*EXCLUDE [2]							

Tabla 6: Combinaciones de Autoridades

Es posible definir combinaciones de manera explícita cuando las combinaciones estándar no satisfacen los requerimientos de seguridad de un objeto particular. Por ejemplo, una aplicación puede requerir que los registros de un archivo de transacciones no sean leídos, actualizados o borrados; solamente es válido adicionar registros. En este caso, *OBJOPR y *ADD deben ser especificados, ya que ninguna combinación establecida cumple con los requerimientos.

La Figura 11 presenta el esquema del conjunto total de las autoridades existentes en el AS/400.

[2] *EXCLUDE no es la ausencia de autoridad; es una autoridad que previene el acceso a un objeto.

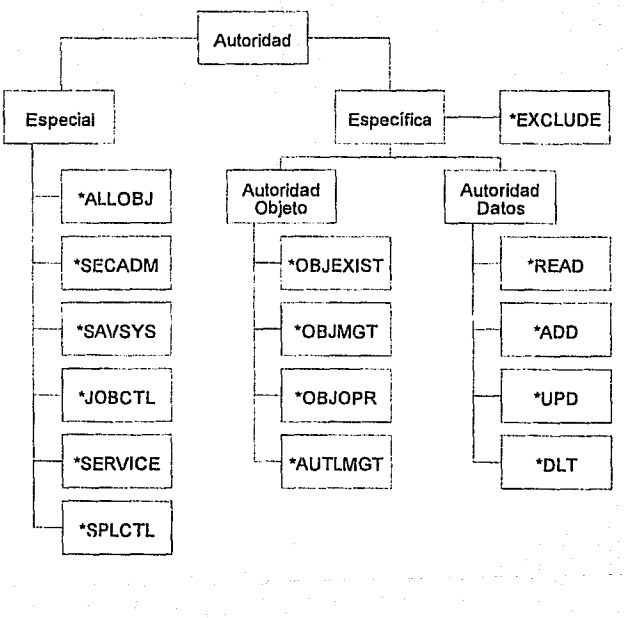


Figura 11: Autoridades del Sistema

4.8 Portadores de Autoridad

Otro objeto de seguridad es el portador de autoridad, una herencia del S/36. Su único propósito es permitir que una aplicación borre y regenere archivos sin perder las autoridades asociadas a ellos. Su uso se relaciona casi siempre con aplicaciones provenientes de un S/36. Es un objeto sin datos que recibe el mismo tratamiento que un archivo de datos. Cuando un programa genera un archivo con el mismo nombre que el portador de autoridad, todas las autoridades asociadas al portador son transferidas automáticamente al archivo. De la misma manera, cuando este archivo es borrado, las autoridades son regresadas al portador de autoridad.

4.9 Autoridad Pública

Todo objeto tiene una autoridad pública definida. Esta es la autoridad que poseen todos los usuarios que no cuentan con autoridad específica (privada) sobre el objeto. La autoridad pública se establece con los comandos de creación (CRTxxx) del OS/400 y puede cambiarse con los comandos de otorgamiento y revocación de autoridades (GRTOBJAUT y RVKOBJAUT). En la generalidad de los casos, el sistema define implícitamente autoridades públicas iguales a *CHANGE para casi todos los objetos creados. Los perfiles de usuario son una excepción, ya que son creados con la autoridad pública *EXCLUDE.

El uso de la autoridad pública reduce sustancialmente la necesidad de asignar autoridades específicas sobre los objetos, tanto individuales como de grupo. Si un archivo no es confidencial y toda la organización requiere leerlo, la autoridad pública sobre este objeto debe ser *USE. Esto resulta ser más eficiente que asignarle la autoridad pública *EXCLUDE y otorgar autoridad específica *READ a todos los individuos que soliciten acceso al archivo.

El propósito fundamental del concepto de autoridad pública es reducir el número de autoridades existentes en el sistema y simplificar las tareas de administración de autoridades específicas sobre objetos. Sin embargo, también debe considerarse tan cuidadosamente como otros aspectos de seguridad.

4.10 Propiedad Individual y Grupal

Todo objeto tiene un solo propietario. El nombre del propietario es siempre el nombre de un perfil de usuario, un user-id. El propietario es muy importante debido a que generalmente controla el acceso a sus objetos. Dicho control se presenta a partir de las autoridades que el propietario otorga a otros usuarios demandantes

de acceso. El oficial de seguridad u otros usuarios con *ALLOBJ pueden, desde luego, autorizar a otros usuarios. Sin embargo, este no es el método común para crear autoridades.

El propietario puede limitar temporalmente su propia autoridad para evitar daños accidentales a sus objetos. Asimismo, puede delegar la responsabilidad de autorizar el acceso, al otorgar la autoridad *OBJMGT a otro individuos.

Un perfil de grupo también puede ser propietario de objetos. En este caso, los miembros corrientes de un grupo comparten el privilegio de propiedad, la autoridad *ALL sobre los objetos del grupo. Lo mismo sucede con las autoridades específicas que han sido otorgadas al perfil de grupo por otros usuarios. Cuando un usuario es removido del grupo, todas las autoridades que hereda del grupo son canceladas automáticamente. La integración de nuevos miembros al grupo también permite que éstos reciban el privilegio de propiedad.

En algunas ocasiones el miembro de un grupo puede ser el propietario de ciertos objetos. Cuando esto se presenta, el miembro puede transferir o no la autoridad *ALL y otras autoridades específicas al grupo que pertenece. Los valores presentes en los parámetros OWNER y GRPAUT, contenidos en el perfil de usuario del miembro, determinan en buena medida qué autoridades hereda el grupo en cuestión.

4.11 Listas de Autorización

Una lista de autorización es otro objeto de seguridad importante proveniente del S/36. Permite relacionar un conjunto de usuarios con un grupo de objetos, a través de la definición de autoridades específicas. Un objeto sólo puede asociarse a una lista de autorización, pero una lista puede incluir múltiples objetos. Un usuario puede aparecer en diferentes listas.

Las listas de autorización no son afectadas con el borrado de los objetos referenciados. Si un objeto es borrado y restaurado posteriormente en el sistema, éste es ligado automáticamente a la lista de autorización que lo incluye. Este hecho representa una consideración importante en el uso de listas de autorización.

Las funciones de los perfiles de grupo y las listas de autorización suelen traslaparse. La Figura 12 ilustra la distinción entre unos y otras.

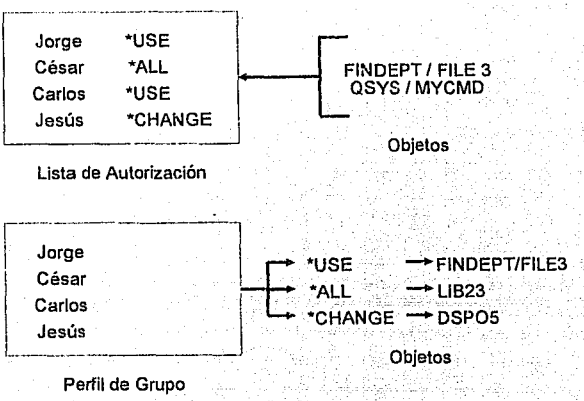


Figura 12: Lista de Autorización vs. Perfil de Grupo

En una lista de autorización, cada usuario puede tener niveles distintos de autoridad. Estos niveles de acceso aplican por igual a todos los objetos protegidos por la lista. En un perfil de grupo, todos sus miembros mantienen el mismo nivel de autoridad sobre un objeto en particular.

4.12 Búsqueda de Autorizaciones

El AS/400 define un orden estricto de búsqueda de elementos de autorización para conceder el acceso de un usuario a un objeto. Esta secuencia establece la existencia de varias condiciones prevalecientes entre el usuario y el objeto. Resulta muy importante entender que la primera ocurrencia de una de estas condiciones es la que el sistema adopta. Es posible que algunas otras condiciones también se cumplan; sin embargo, la primera es la que se utiliza. Si un usuario tiene varias

autorizaciones hacia un objeto, el sistema no necesariamente selecciona la más alta. Asume la primera de ellas en el recorrido de búsqueda, sin importar su nivel. El acceso es denegado, desde luego, si no se cumple alguno de estos criterios.

Este es el orden de búsqueda utilizado por el AS/400. Se asume que un usuario demanda acceso a un objeto en particular.

a) ¿Tiene el usuario la autoridad especial *ALLOBJ ?

b) ¿Tiene el usuario autoridad específica sobre el objeto ?

c) ¿ Está el usuario en alguna lista de autorización asociada con el objeto ?

d) ¿Tiene el grupo del usuario la autoridad especial *ALLOBJ ?

e) ¿Tiene el grupo del usuario autoridad especifica sobre el objeto ?

f) ¿ Está el grupo del usuario en alguna lista de autorización asociada con el objeto ?

g) ¿La autoridad pública del objeto satisface el requerimiento de acceso del usuario ?

h) ¿La autoridad pública señalada en alguna lista de autorización asociada con el objeto satisface el requerimiento de acceso del usuario ?

4.13 Autoridad Adoptiva

La autoridad adoptiva es una facilidad de seguridad del AS/400 muy importante. Un programa de usuario y un comando del sistema operan normalmente al nivel de autoridad del usuario que los invoca. Por tanto, el mismo programa puede ser ejecutado a distintos niveles de autoridad, dependiendo de quién los utiliza.

Esto no siempre es conveniente, si consideramos que ciertos programas o comandos requieren mayor autoridad que la que se encuentra disponible para el usuario que necesita utilizarlos. El AS/400 ofrece una alterantiva para este problema, llamada autoridad adoptiva.

Este esquema permite a un usuario adoptar la autoridad del propietario de un programa durante su ejecución, en conjunto con sus propias autoridades. La ventaja del uso de este concepto es que los usuarios pueden accesar los archivos direccionados por un programa de aplicación, sin la necesidad de otorgarles autoridad directa sobre estos objetos. Se asume, desde luego, que el propietario posee una mayor autoridad que los usuarios normales.

La autoridad adoptada tiene buenos y malos aspectos. Cuando su control es adecuado, adiciona una función poderosa al sistema. Sin embargo, la inspección y control de todos los programas que utilizan esta facilidad puede llegar a representar una tarea demasiado complicada. Algunos riesgos se presentan cuando el propietario de algunos programas cuenta con la autoridad *ALLOBJ y también en los casos en que un programa que adopta autoridad llama a otros programas via la función CALL.

4.14 Valores del Sistema

El AS/400 cuenta con una variedad de valores del sistema, variables que permiten adaptar muchas de las características y funciones del equipo a las necesidades particulares de la organización. Algunas de estos valores controlan diversos aspectos relacionados con la seguridad. Es indispensable contar con las autoridades especiales *ALLOBJ y *SECADM para trabajar con ellos. La Tabla 7 describe brevemente algunos de estos parámetros de seguridad. Las opciones que adopta el sistema por omisión aparecen subrayadas.

4.15 Administración de Passwords

El AS/400 posee facilidades que alientan una administración adecuada de los passwords de los usuarios. En particular, existen una serie de valores del sistema cuyo uso garantiza la rotación oportuna de estas claves, evita su reciclamiento en el sistema y procura el manejo de palabras no triviales de longitud adecuada. La Tabla 8 describe todos éstos. Las opciones que adopta el sistema por omisión aparecen subrayadas.

Nombre	Descripción	Valores Posibles	Valor Recomendado
QSECURITY	Determina el nivel de seguridad bajo el que opera el sistema.	10, 20, 30 ó 40	30 ó 40
QAUDLVL	Determina la naturaleza de los eventos que son registrados en la bitácora de auditoría del sistema (QAUDJRN).	*NONE La función de auditoría no se encuenta habilitada. *AUTFAIL Registro de fallas de autoridad. *CREATE Registro de operaciones de creación. *DELETE Registro de operaciones de borrado. *OBJMGT Registro de operaciones de movimiento y renombrado. *PGMFAIL Registro de violaciones de integridad. *SAVRST Registro de operaciones de restauración. *SECURITY Registro de funciones de seguridad.	La combinación de valores requerida.
QDSPSGNINF	Determina si la pantalla de información de sign-on es desplegada después de la firma exitosa de un usuario. Dicha pantalla señala lo siguiente: • Fecha de la última firma • Intentos frustrados de firma • Número de días por transcurrir para la expiración del password	0 La pantalla no es desplegada. 1 La pantalla es desplegada	1

Tabla 7: Valores del Sistema (Seguridad)

Nombre	Descripción	Valores Posibles		Valor Recomendado
QMAXSIGN	Controla el número permitido de intentos incorrectos de sign-on consecutivos. Estos pueden originarse a partir de user-id's y passwords incorrectos o de la falta de autoridad en el uso de una terminal.	15 *NOMAX Límite	Se permiten 15 intentos de sign-on incorrectos. El sistema permite un número ilimitado de intentos de firma. Un número en el rango de 1 hasta 25.	3
QMAXSGNACN	Determina la acción realizada por el sistema después de alcanzar el límite establecido por el valor QMAXSIGN.	3 Deshabilitar el perfil y la terminal. 2 Deshabilitar el perfil de usuario. 1 Deshabilitar la terminal.		3
QINACTITV	Especifica, en minutos, el período de inactividad permitida en trabajos interactivos.	*NONE Intervalo (minutos)	El sistema no verifica períodos de inactividad. Un número entre 5 y 300.	15
QINACTMSGQ	Determina la acción realizada por el sistema después de alcanzar el intervalo definido en QINACTITV.	*ENDJOB *DSCJOB Cola de mensajes	Los trabajos inactivos son terminados. Los trabajos inactivos son desconectados (suspendidos). El mensaje CPI1126 es enviado a la cola de mensajes especificada.	*DESCJOB

Tabla 7: Valores del Sistema (Seguridad)

Nombre	Descripción	Valores Posibles	Valor Recomendado
QLMTSECOFR	Limita el acceso de usuarios con *ALLOBJ o *SERVICE a terminales.	1 Los usuarios con *ALLOBJ y * SERVICE pueden firmarse únicamente a terminales sobre las que poseen autoridad especifica. 0 Los usuarios con *ALLOBJ y *SERVICE pueden firmarse a cualquier terminal con autoridad pública *CHANGE.	1
QLMTDEVSSN	Determina el número de sesiones interactivas simultáneas que un usuario puede mantener en distintas terminales.	0 El sistema permite un número ilimitado de sesiones concurrentes en distintas terminales. 1 Los usuarios están limitados a una sola sesión.	1

Tabla 7: Valores del Sistema (Seguridad)

Nombre	Descripción	Valores Posibles	Valor Recomendado
QPWDEXPITV	Define el intervalo de expiración de passwords.	*NOMAX No se requiere que los usuarios cambien sus passwords. Días Un valor en el rango de 1 a 366.	30
QPWDMINLEN	Controla el número mínimo de caracteres requeridos en el password.	1 Un mínimo de un caracter se requiere. Número Un valor en el rango de 1 a 10.	6
QPWDMAXLEN	Controla el número máximo de caracteres permitidos en el password.	10 Un máximo de 10 caracteres pueden utilizarse. Número Un valor en el rango de 1 a 10.	8
QPWDRQDDIF	Determina si un password nuevo debe ser distinto a los 32 anteriores.	0 No se requieren passwords distintos. 1 El password no puede ser igual a alguno de los 32 anteriores.	1
QPWDLMTCHR	Limita el uso de ciertos caracteres en el password.	*NONE Cualquier caracter puede utilizarse. Caracteres Una cadena de caracteres restringidos.	A, E, I, O y U
QPWDLMTAJC	Limita el uso de caracteres numéricos adyacentes en el password.	0 Se permiten caracteres numéricos adyacentes. 1 No se permiten caracteres numéricos adyacentes.	1
QPWDLMTREP	Limita el uso de caracteres repetidos en el password.	0 Se permite la repetición de caracteres. 1 No se permite la repetición de caracteres.	1
QPWDPOSDIF	Controla la definición de un password con los mismos caracteres en las mismas posiciones que el password anterior.	0 Se pueden utilizar los mismos caracteres en las mismas posiciones. 1 No se pueden utilizar los mismos caracteres en las mismas posiciones.	1
QPWDRQDDGT	Controla la existencia de caracteres numéricos en el password.	0 No se requieren caracteres numéricos. 1 Se requiere al menos un caracter numérico.	1

Tabla 8: Valores del Sistema (Gestión de Passwords)

4.16 Uso de Comandos

Los comandos son objetos y tienen autorizaciones. El sistema proporciona autorizaciones apropiadas para varios comandos. El acceso a ellos depende en buena medida de las autoridades especiales asignadas al usuario y de la autoridad pública señalada en los comandos. El oficial de seguridad o cualquiera con *ALLOBJ puede cambiar estas autoridades. Esta tarea incluye generalmente cambiar la autoridad pública del comando de *USE a *EXCLUDE y luego otorgar autoridad específica a ciertos usuarios. Resulta evidente que estos cambios requieren un análisis previo, ya que pueden tener repercuciones negativas.

4.17 Uso de Terminales

Las terminales son consideradas también objetos, gracias a las descripciones de dispositivo que tienen asociadas. Al igual que con otros objetos, es posible limitar su uso a ciertos usuarios a través de autoridades específicas, listas de autorización, perfiles de grupo y autoridades públicas.

Adicionalmente, las terminales del AS/400 están equipadas con cerraduras de seguridad que evitan la entrada y el despliege de datos.

Capítulo 5

5. Niveles de Seguridad

El AS/400 puede operar a cuatro niveles distintos de seguridad: 10, 20, 30 y 40. La Tabla 9 muestra la comparación de estos niveles.

Función	Nivel 10	Nivel 20	Nivel 30	Nivel 40
Sign-on requiere user-id	SI	SI	SI	SI
Sign-on requiere password	NO	SI	SI	SI
Seguridad de passwords activa	NO	SI	SI	SI
Seguridad de menú y programa inicial activa	NO	SI [3]	SI [3]	SI [3]
Soporte de capacidades limitadas activo	NO	SI	SI	SI
Seguridad de recursos activa	NO	NO	SI	SI
Acceso a todos los objetos	SI	SI	NO	NO
Creación automática de perfiles de usuario	SI	NO	NO	NO
Los programas que utilizan instrucciones restringidas no pueden crearse o recompilarse	SI	SI	SI	SI
Los programas que utilizan interfases no soportadas no pueden ser ejecutados	NO	NO	NO	SI
Protección de almacenamiento por hardware	NO	NO	NO	SI

Tabla 9: Comparación de Niveles de Seguridad

El valor de la variable del sistema QSECURITY determina, en todo momento, el nivel de seguridad utilizado en la operación del sistema. El comando WRKSYSVAL permite la modificación de estos niveles, siempre y cuando el usuario que lo utilice cuente con las autoridades *ALLOBJ y *SECADM. Cualquier cambio de nivel tiene efecto únicamente después de correr un IPL (Initial Program Load).

Inicialmente, IBM entrega el sistema a su clientela en el nivel 10. Después de instalado, debe migrarse de inmediato a un nivel 20 o superior, a fin de fortalecer la seguridad. El nivel 30 es altamente recomendable, en virtud de que no concede a los usuarios acceso irrestricto a todos los recursos almacenados. Las instalaciones con requerimientos de seguridad muy elevados deben utilizar el nivel 40.

---

[3] Cuando se especifica LMTCPB (*YES) en el perfil de usuario.

Durante la creación de perfiles de usuario, el nivel de seguridad determina qué autoridades especiales se asocian implícitamente a cada clase de usuario. Estas autoridades también son cambiadas y removidas cuando se modifica el nivel. Las Tablas 4 y 5 del capítulo 4 muestran la asignación de autoridades por clase de usuario a distintos niveles de seguridad.

5.1 Nivel de Seguridad 10

La seguridad es mínima a nivel 10. Cuando un usuario se firma, el sistema crea un perfil de usuario con el nombre del user-id proporcionado en la pantalla de sign-on. Si el usuario repite posteriormente el proceso de conexión con un user-id distinto, se genera un nuevo perfil. El contenido de los perfiles así creados se determina a partir de una serie de valores por omisión definidos para el nivel 10.

El sistema verifica autoridades a todos los niveles de seguridad. En el nivel 10, los usuarios aprueban cualquier revisión y tienen acceso a todos los recursos. Esto se debe a que todos los perfiles de usuario creados bajo este nivel reciben la autoridad *ALLOBJ.

5.2 Nivel de Seguridad 20

El nivel 20 proporciona las siguientes funciones de seguridad adicionales:

- El sign-on de los usuarios requiere de user-id y password.
- Unicamente el oficial de seguridad o alguien con *SECADM puede crear perfiles de usuario.
- La función de limitar las capacidades de los usuarios puede activarse desde los perfiles de usuario.

Todos los perfiles de usuario creados automáticamente en el nivel 10 se preservan al migrar al nivel 20. El password en cada uno de éstos es igual al nombre del perfil. Ningún cambio se realiza sobre las autoridades especiales asignadas.

La siguiente lista representa una serie de acciones recomendadas para migrar al nivel 20 desde el nivel 10:

- Listar todos los perfiles de usuario en el sistema con el comando DSPAUTUSR.
- Copiar los perfiles existentes con nombres estandarizados.
- Expirar los passwords en cada uno de los perfiles para forzar a los usuarios a cambiarlos.
- Utilizar los valores del sistema que regulan la composición de passwords.
- Revisar el contenido de la información de los perfiles creados en el nivel 10 y realizar los cambios pertinentes.

En los casos en que el cambio de nivel de seguridad proceda de un nivel superior hacia los niveles 10 o 20, ciertas autoridades especiales son adicionadas o removidas para satisfacer las reglas de asociación señaladas en la Tabla 4. La autoridad *ALLOBJ es asignada en cualquier caso.

5.3 Nivel de Seguridad 30

El nivel de seguridad 30 ofrece dos ventajas sustanciales en adición a las observadas bajo el nivel 20. Estas son:

- Se deben otorgar autoridades específicas a los usuarios del sistema para usar los recursos en el sistema (seguridad de recursos).
- La autoridad *ALLOBJ se asigna de manera implícita únicamente a los perfiles de usuario de clase *SECOFR.

La adopción del nivel 30 desde un nivel de seguridad inferior incluye cambios a los perfiles de usuario. Una vez más, las autoridades especiales son modificadas tal y como lo establece la Tabla 5. Por ejemplo, *ALLOBJ es removida de todos los perfiles, a excepción de aquellos con clase *SECOFR.

Resulta indispensable establecer y probar la seguridad de recursos antes de implantar el nivel 30 desde niveles inferiores, sobre todo, cuando se han utilizado diversas aplicaciones por algún tiempo. Se recomienda desarrollar las siguientes acitividades:

- Establecer autoridades apropiadas sobre los objetos de cada aplicación.
- Utilizar perfiles existentes o de prueba para verificar el comportamiento de las aplicaciones:
  - Remover *ALLOBJ de los perfiles usados.
  - Otorgar a los perfiles autoridades pertinentes sobre los objetos de aplicación.
  - Correr las aplicaciones con estos perfiles.
  - Monitorear la ocurrencia de fallas de autoridad en mensajes de error o en la bitácora de auditoría (QAUDJRN).
- Otorgar a los perfiles "productivos" las autoridades requeridas sobre los objetos, una vez que las aplicaciones corran satisfactoriamente con los perfiles de prueba.
- Cambiar el nivel de seguridad del sistema y ejecutar un IPL.

5.4 Nivel de Seguridad 40

En algunos casos especiales, ciertos programas pueden circunvenir la seguridad establecida. El nivel de seguridad 40 procura un mayor nivel de intregridad y protección, al prevenir la materialización de los riesgos potenciales planteados por estos programas.

A niveles inferiores de seguridad, el sistema mantiene registros de auditoría sobre el uso de este tipo de programas. En el nivel 40, estas violaciones a la integridad son registradas y también evitadas. Este último hecho representa, la ventaja más significativa de este nivel de seguridad. Debe asumirse que la función de auditoria provista por el valor del sistema QAUDLVL está activa.

La migración al nivel 40 supone que todas las aplicaciones corren satisfactoriamente bajo el nivel 30. El siguiente procedimiento puede utilizarse para la implantación del nivel 40:

- Activar la bitácora QAUDJRN y especificar los valores *AUTFAIL y *PGMFAIL en la variable del sistema QAUDLVL.
- Monitorear el contenido de QAUDJRN durante la ejecución de las aplicaciones bajo el nivel 30 e identificar los registros con códigos AF de tipo B, C, D, J, R y S. Estos representan riesgos de integridad en las aplicaciones. Estos programas no podrán correr en el nivel 40.
- Corregir los programas de las aplicaciones que generan estas violaciones de integridad.
- Cambiar el valor del sistema QSECURITY a 40 y ejecutar un IPL.

Frecuentemente es necesario retornar al nivel 30 para probar nuevas aplicaciones o corregir algunas anomalías que no fueron detectadas con anterioridad. En ambos casos, no existe problema alguno, ya que la seguridad de los recursos no se ve comprometida y las autoridades especiales no son modificadas.

5.4.1 Uso de Interfases no Soportadas

Al nivel 40, el sistema previene cualquier intento por llamar directamente programas del sistema que no han sido documentados como interfases de "nivel de llamado" (call-level). Dos atributos, el dominio del objeto y el estado del programa, se utilizan para lograr este tipo de protección.

Todo objeto pertenece al dominio *SYSTEM o al dominio *USER. Los objetos del dominio *SYSTEM pueden ser accesados únicamente por programas del estado *SYSTEM. El comando DSPOBJD con el parámetro DETAIL(*FULL) se utiliza para identificar el dominio de un objeto.

De la misma manera, un programa pertenece al estado *SYSTEM o al estado *USER. Los programas del estado *USER pueden accesar objetos del dominio *USER. Los objetos *SYSTEM pueden accesarse a través del uso de comandos o por las interfases de programación aplicativa soportadas (API's). El estado *SYSTEM está reservado para programas de IBM. El atributo de estado de un programa puede identificarse con el comando DSPPGM.

La Tabla 10 muestra las reglas de acceso determinadas por los conceptos de dominio de objetos y estado de programas.

	Dominio	
Estado	*USER	*SYSTEM
*USER	SI	NO
*SYSTEM	SI	SI

Tabla 10: Acceso por Dominio y Estado

Todo intento de uso de una interfase no soportada es suspendido y registrado en la bitácora de auditoría QAUDJRN, como una violación AF del tipo D.

5.4.2 Uso de Instrucciones Restringidas

El uso del nivel 40 impide el acceso a estructuras internas del sistema desde lenguajes equipados con facilidades para el manejo de apuntadores, tales como C/400, Pascal o Ensamblador. Este tipo de operaciones se registran como violaciones AF del tipo B en QAUDJRN.

5.4.3 Protección de Descripciones de Trabajos

Un trabajo puede ejecutarse con los atributos de un perfil de usuario, si en el campo de usuario de la descripción del trabajo se incluye el nombre de ese perfil. En este sentido, algunas violaciones a la seguridad pueden presentarse cuando un usuario no autorizado utiliza dicha descripción para correr el trabajo con privilegios que no le corresponden.

En el nivel 40, esta operación no puede realizarse, a menos que el usuario que pretende ejecutar el trabajo cuente con autoridad *USE sobre la descripción del trabajo y el perfil de usuario referenciado. De no cumplirse estas condiciones, la operación es interrumpida desde un inicio y se registra la violación AF tipo J en QAUDJRN.

5.4.4 Sign-on sin Password

En el nivel 30, es posible firmarse sin user-id y password con el uso de las descripciones de ciertos subsistemas. El nivel 40 detiene estos sucesos y registra una violación AF tipo S.

5.4.5 Protección de Almacenamiento por Hardware

La protección de almacenamiento por hardware permite que ciertos bloques de información del sistema localizados en disco puedan definirse como de lectura/escritura, de sólo lectura o no accesibles. El nivel de seguridad 40 controla el acceso de programas de estado *USER a estas áreas protegidas. Esta facilidad no se encuentra disponible en niveles inferiores de seguridad y en los modelos AS/400 que se enumeran a continuación:

- Todos los modelos de la serie B
- Todos los modelos de la serie C
- Los modelos 9402 D04, 9402 D06, 9404 D10 y 9404 D20 de la serie D.

Todo intento de un programa por escribir en áreas de disco protegidas por este mecanismo de seguridad genera una violación AF del tipo R.

5.4.6 Validación de Programas Restaurados

Desde la Versión 1 Release 3 (V1R3) del OS/400, un programa con instrucciones restringidas no puede ser compilado o creado en un equipo AS/400. En el caso de programas que son restaurados, el sistema utiliza una técnica llamada validación de programas para determinar si éstos contienen instrucciones restringidas.

Durante la creación de un programa bajo V1R3 o superior, el sistema calcula un valor de validación que es almacenado junto con el programa. Cuando este programa es restaurado, dicho valor es recalculado y comparado con el que se encuentra almacenado.

Si ambos son iguales, la restauración tiene éxito. De lo contrario, se realizan una serie de acciones en función del nivel de seguridad establecido y del parámetro ALWOBJDIF del comando RSTOBJ. Estas acciones pueden ser:

- Intentar crear de nuevo el programa.
- Registrar una entrada en QAUDJRN.
- Enviar un mensaje a la bitácora de trabajos.
- Asignar la propiedad del programa al perfil QDFTOWN.
- Revocar la autoridad del programa restaurado.

Capítulo 6

6. Perfiles de Usuario

Este capítulo explica el propósito y las características de los elementos de seguridad presentes en los perfiles de usuario del AS/400. Como se ha mencionado anteriormente, estos objetos especiales constituyen el eje de la seguridad en estas plataformas de hardware. Este hecho realza la importancia de comprender la información que se incluye en los apartados que siguen.

6.1 Roles del Perfil de Usuario

En la generalidad de los casos, todo perfil de usuario juega varios roles en el sistema:

- Contiene información de seguridad que controla el sign-on del usuario y las acciones que éste puede desarrollar después de su identificación y autentificación.
- Contiene información diseñada para customizar el sistema y adaptarlo al usuario.
- Es una herramienta de administración y recuperación para el sistema operativo, ya que incluye información sobre los objetos propiedad del usuario y todas las autoridades privadas sobre éstos.
- El nombre del perfil identifica los trabajos y las salidas impresas del usuario.

El sistema crea automáticamente un perfil de usuario cuando alguien se firma al sistema con un user-id que no existe y el nivel de seguridad es 10. A un nivel superior, el perfil debe existir antes del sign-on de un usuario.

6.2 Campos del Perfil de Usuario

La información almacenada en los perfiles se encuentra organizada en campos, cuyo contenido determina la capacidad de interación del usuario con el sistema. Las siguientes descripciones se refieren exclusivamente a aquellos campos con relevancia para la seguridad. Para cada uno de ellos se incluye una explicación de su funcionamiento, el nombre del parámetro de CL asociado y, en los casos pertinentes, posibles valores y recomendaciones. Los valores que adopta el sistema implícitamente aparecen subrayados.

6.2.1 Nombre del Perfil de Usuario (USRPRF)

El nombre del perfil de usuario permite que el sistema identifique al usuario. Se le conoce también como el user-id y es el nombre que el usuario proporciona durante el proceso de sign-on. Su longitud máxima es de 10 caracteres. Estos pueden extraerse de los siguientes conjuntos:

- Cualquier letra (A - Z)
- Cualquier número (0 - 9)
- Los símbolos #, $, @ y _

Ningún nombre puede comenzar con un número. Es posible que un usuario se firme con un user-id numérico, siempre y cuando el nombre del perfil sea creado con la letra Q como primer caracter. Por ejemplo, el nombre Q12345 permite firmas con 12345 o Q12345.

El sistema no distingue entre letras mayúsculas y minúsculas. Cualquier caracter en minúsculas ingresado desde una terminal es traducido a mayúsculas por el sistema.

Una técnica disponible para asignar nombres de perfiles consiste en utilizar los primeros siete caracteres del apellido y la primera letra del nombre propio de un usuario. En el caso de perfiles de grupo, es necesario utilizar una nomenclatura que procure una fácil identificación. Por ejemplo, las cadenas GRP o DPT pueden usarse como los primeros caracteres del nombre, ya que designan un grupo de usuarios o un departamento de la organización con necesidades de acceso similares.

6.2.2 Password (PASSWORD)

El password se utiliza para verificar la identidad de un usuario (autentificación). El user-id y el password siempre deben especificarse durante el sign-on, cuando el valor del sistema QSECURITY es igual o mayor a 20.

Los valores del sistema QPWDMINLEN y QPWDMAXLEN gobiernan las longitudes mínima y máxima de los passwords. Sin embargo, la longitud máxima no puede sobrepasar los 10 caracteres. Las reglas de especificación de passwords son las mismas que se utilizan para nombrar perfiles de usuario.

El almacenamiento de passwords supone el uso de técnicas unidireccionales de encripción. No se cuenta con método alguno para decodificarlos. Si un password se olvida, el oficial de seguridad puede utilizar el comando de modificación de perfiles de usuario (CHGUSRPRF) para asignar un password temporal y forzar su expiración. Estas acciones obligan al usuario a cambiar este password durante su siguiente sign-on.

Algunos de los valores del sistema descritos en el Capítulo 4 pueden utilizarse para controlar la composición de los passwords que los usuarios definen. Cabe señalar que estos valores tienen efecto únicamente cuando el cambio de password se realiza con el comando CHGPWD, el menú ASSIST o la API denominada QSYCHGPW. El uso de cuando menos una de estas variables impide, además, la asignación de passwords iguales a los nombres de los perfiles.

Cuando el password se modifica a través del comando CHGUSRPRF, los valores del sistema utilizados no son considerados por el sistema. Esta característica permite que un usuario con *SECADM realice las acciones correctivas pertinentes ante el olvido de passwords.

Valores Posibles:

- *USRPRF — El password para este usuario es igual al nombre de su perfil.
- *NONE — Ningún password se asigna a este perfil. A nivel de seguridad 20 o superior, no se permite sign-on alguno.
- *Password* — Una cadena alfanumérica de caracteres.

Recomendaciones:

- Utilizar el valor *NONE en perfiles de grupo para evitar sign-on's a ellos.
- Establecer un password inicial durante la creación de un perfil individual y obligar al usuario a cambiarlo en su próximo sign-on.
- Usar los valores del sistema pertinentes para evitar el uso de passwords triviales y garantizar su rotación periódica.

6.2.3 Expiración de Passwords (PWDEXP)

Este campo permite al administrador de la seguridad indicar que el password ha expirado y debe ser cambiado en el siguiente intento de sign-on del usuario. Muy a menudo, se utiliza durante la creación de perfiles de usuario o ante el olvido de passwords. En ambos casos, alienta la modificación del password temporal asignado por el encargado de la seguridad. Este hecho reduce riesgos, al evitar que este personaje conozca los passwords de los usuarios.

Cuando el password expira, el usuario recibe un mensaje en la pantalla de sign - on que demanda el cambio de su password. Se puede oprimir la tecla de Enter para asignar un nuevo password o la tecla F3 para cancelar el intento de sign-on. En el primer caso, se muestra el desplegado del comando CHGPWD.

Valores Posibles:

- *NO — El password está vigente.
- *YES — El password expira y debe ser modificado.

Recomendaciones:

PWDEXP (*YES) debe usarse durante la creación de un perfil o cuando se asigna un password temporal.

6.2.4 Status (STATUS)

El valor de este campo determina si el perfil se encuentra habilitado o deshabilitado. En el primer caso, es posible firmarse al perfil. En el segundo, un usuario autorizado tiene que activar el perfil para poder utilizarlo.

El comando CHGUSRPRF se puede utilizar para habilitar un perfil. Se debe contar con la autoridad especial *SECADM y las autoridades específicas *OBJMGT y *USE sobre el perfil para lograr esto.

El sistema puede deshabilitar un perfil después de cierto número de intentos frustrados de sign-on, tal y como lo indican los valores de las variables del sistema QMAXSIGN y QMAXSGNACN.

Siempre es posible firmarse con el perfil QSECOFR desde la terminal designada como consola del sistema, aunque se encuentre deshabilitado. Para lograr su activación basta con ejecutar el comando CHGUSRPRF QSECOFR STATUS(*ENABLED) en la consola.

Valores Posibles:

- *ENABLED El perfil puede usarse para sign-on.
- *DISABLED El perfil no puede usarse para sign-on.

Recomendaciones:

El valor *DISABLED debe utilizarse cuando algún usuario permanecerá fuera de la organización por un periodo prolongado de tiempo.

6.2.5 Clase de Usuario (USRCLS)

La clase de usuario se usa para controlar qué opciones de menú se muestran al usuario. Esto no necesariamente limita el uso de comandos.

Cuando ninguna autoridad especial es especificada durante la creación de un perfil de usuario, la clase y el nivel de seguridad establecido en QSECURITY determinan la asignación de estas autoridades al usuario. Las Tablas 4 y 5 mostradas en el Capítulo 4 señalan las combinaciones disponibles de clase y autoridades a distintos niveles de seguridad.

Valores Posibles:

- *SECOFR Oficial de Seguridad.
- *SECADM Administrador de la Seguridad.
- *PGMR Programador.
- *SYSOPR Operador del Sistema.
- *USER Usuario Final.

Recomendaciones:

La mayoría de usuarios no requieren desarrollar funciones especializadas dentro del sistema. Por tal motivo, resulta conveniente asignarles la clase *USER.

6.2.6 Biblioteca Actual (CURLIB)

La biblioteca actual siempre es analizada antes que las bibliotecas referenciadas en la lista de bibliotecas (*LIBL), durante la búsqueda de objetos que requieren ser accesados por el usuario. De la misma manera, si el usuario crea objetos y especifica *CURLIB, éstos son depositados en la biblioteca actual.

El nombre de esta biblioteca se adiciona automáticamente a la lista del usuario cuando se firma al sistema. No se necesita incluirla en la lista inicial de bibliotecas de la descripción del trabajo del usuario.

El usuario no puede modificar su biblioteca actual si el campo de limitar capacidades en su perfil contiene el valor *YES.

Valores Posibles:

- *CRTDFT — Este usuario no tiene una biblioteca actual. La biblioteca QGPL es utilizada como la biblioteca actual si se especifica *CURLIB al crear objetos.
- *Nombre* — El nombre de la biblioteca actual del usuario. Se requiere contar con autoridad *USE sobre esta biblioteca para poder especificarla en el perfil.

Recomendaciones:

*CURLIB debe utilizarse para controlar el lugar en el que deben ser depositados los objetos creados por el usuario.

6.2.7 Programa Inicial (INLPGM)

Es posible especificar e invocar un programa durante el sign-on de un usuario con el uso de este campo. La ejecución de este programa siempre antecede al desplegado del menú inicial, en los casos en que éste último también sea especificado. Cuando el campo de capacidades limitadas en el perfil contiene el valor *YES, el usuario no puede modificar el nombre del programa inicial en la pantalla de sign-on.

Siempre se requiere contar con la autoridad *USE sobre el programa y *READ sobre la biblioteca que lo contiene, para poder especificar el nombre del programa inicial.

Los programas iniciales se utilizan para dos propósitos principales:

- Restringir al usuario a conjuntos específicos de funciones.
- Realizar algunas operaciones iniciales durante el proceso de firma, tales como abrir archivos o establecer la lista de bibliotecas.

No es posible transferir parámetros al programa inicial. Si éste falla, el usuario no puede conectarse al sistema.

Valores Posibles:

- *NONE — Ningún programa se invoca durante el sign-on. Si se ha especificado el nombre de un menú inicial, éste es desplegado.
- *Nombre* — El nombre del programa que es llamado cuando el usuario se firma.

Existen también las siguientes opciones en la especificación de la biblioteca del programa inicial:

- *LIBL — La lista de bibliotecas es utilizada para localizar el programa. Si la descripción del trabajo especificada en el perfil del usuario contiene el nombre de una lista inicial de bibliotecas, ésta es la que se se usa. Cuando dicha descripción contiene *SYSVAL, el valor de la variable del sistema QUSRLIBL determina la lista que contiene al programa.
- *CURLIB — La biblioteca actual es la que se utiliza para localizar el programa inicial. Si no se ha definido la biblioteca actual, QGPL se usa para este propósito.
- *Nombre* — El nombre de la biblioteca en la que reside el programa.

6.2.8 Menú Inicial (INLMNU)

Se puede especificar también el nombre de un menú inicial que se muestra justo después del término de la ejecución del programa inicial.

Si se desea correr únicamente el programa inicial, debe señalarse *SIGNOFF como menú inicial.

El usuario no puede modificar el menú inicial mostrado en la pantalla de conexión al sistema, cuando el campo de capacidades limitadas en el perfil del usuario contiene *YES. En caso contrario, el nombre del menú puede cambiarse y reemplazar al señalado en el perfil correspondiente.

Valores Posibles:

- MAIN — El menú principal del OS/400 es mostrado.
- *SIGNOFF — La sesión del usuario es finalizada cuando el programa inicial termina su ejecución. Esta opción se utiliza para limitar al usuario a un solo programa.
- *Nombre* — El nombre del menú que se invoca durante el proceso de sign-on.

Las opciones de especificación de la biblioteca que contiene el menú inicial son las mismas que para el programa inicial. Sin embargo, el programa inicial puede adicionar bibliotecas a la lista del usuario y ampliar, de esta manera, el rango de búsqueda del menú inicial.

6.2.9 Capacidades Limitadas (LMTCPB)

El campo de capacidades limitadas puede usarse para limitar el ingreso de comandos e impedir el reemplazo del programa inicial, el menú inicial, la biblioteca actual y el programa de atención en la pantalla de conexión al sistema. Representa una importante herramienta de seguridad para prevenir que los usuarios experimenten con el sistema.

Un usuario con capacidades limitadas sólo puede ejecutar comandos que han sido definidos con el valor *YES en el parámetro ALWLMTUSR. Esta característica puede observarse en el siguiente conjunto reducido de comandos, establecido por IBM en las configuraciones iniciales de equipos que distribuye de fábrica a sus clientes.

- Terminar sesión (SIGNOFF)
- Enviar mensaje (SNDMSG)
- Desplegar mensajes (DSPMSG)
- Desplegar trabajo (DSPJOB)
- Desplegar bitácora de trabajos (DSPJOBLOG)
- Iniciar organizador de PC (STRPCO)

El campo LMTCPB en el perfil de usuario y el parámetro ALWLMTUSR en los comandos aplican únicamente sobre comandos que son ejecutados desde la línea de comandos o la pantalla de entrada de comandos. No restringen el uso de comandos en programas de CL.

Existe la posibilidad de permitir al usuario limitado correr comandos adicionales o remover algunos de los comandos de la lista anterior, a través de la modificación del parámetro ALWLMTUSR con el comando CHGCMD. Esta opción también se encuentra presente durante la creación de comandos personales y el uso del comando CRTCMD.

Valores Posibles:

La Tabla 11 muestra los valores posibles para este campo y las funciones permitidas para cada uno de ellos. *NO es el valor implícito utilizado.

	Valores de LMTCPB		
Función	*YES	*PARTIAL	*NO
Cambiar Programa Inicial	No	No	Si
Cambiar Menú Inicial	No	Si	Si
Cambiar Biblioteca Actual	No	Si	Si
Cambiar Programa de Atención	No	No	Si
Ingresar Comandos	Algunos	Si	Si

Tabla 11: Valores de LMTCPB

Recomendaciones:

El manejo de un menú inicial y el uso restringido de la línea de comandos permiten establecer un ambiente de trabajo adecuado para un usuario que no requiere accesar funciones del sistema.

6.2.10 Texto (TEXT)

El campo de texto se utiliza para describir el perfil de usuario o para explicar su propósito. En el caso de perfiles individuales, debe indicarse el nombre del usuario y su departamento. Para perfiles grupales, es necesario identificar los departamentos usuarios contenidos en el grupo.

Valores Posibles:

- *BLANK — Ningún texto es especificado.
- *Descripción* — Una cadena alafanumérica de no más de 50 caracteres.

Recomendaciones:

El campo de texto es truncado en muchos desplegados del sistema. Resulta importante, por tal motivo, escribir la información más relevante al principio del campo.

6.2.11 Autoridad Especial (SPCAUT)

El campo de autoridad especial se utiliza para especificar el tipo de acciones que un usuario puede llevar a cabo sobre los recursos del sistema. El otorgamiento de una autoridad especial a un perfil de usuario requiere que el individuo que la concede cuente con esa misma autoridad. Es posible asignar más de una autoridad especial a un usuario.

Valores Posibles:

El conjunto de autoridades especiales que pueden especificarse en este campo fueron explicadas en el capítulo 4. En adición a *ALLOBJ, *SECADM, *JOBCTL, *SPLCTL, *SAVSYS y *SERVICE, existen dos alternativas más que no son propiamente autoridades.

- *USRCLS — El sistema asigna automáticamente las autoridades especiales de acuerdo al contenido del campo USRCLS y al valor de la variable del sistema QSECURITY. Ninguna otra autoridad puede señalarse.
- *NONE — No se conceden autoridades especiales a este usuario.

Recomendaciones:

- Evaluar cuidadosamente la necesidad de asignar autoridades especiales a un perfil de usuario.
- Monitorear constantemente los perfiles que poseen autoridades especiales y, en los casos pertinentes, también los programas que las adoptan.

6.2.12 Despliegado de Información de Sign-on (DSPSGNINF)

Este campo determina la presentación de la pantalla de información de sign-on durante la firma del usuario. En ella se muestra la fecha del último sign-on, el número de intentos frustrados de firma y el número de días por transcurrir para la expiración del password.

Valores Posibles:

- *SYSVAL — El valor de la variable del sistema QDSPSGNINF es utilizado.
- *NO — La pantalla de información de sign-on no es desplegada.
- *YES — La pantalla de información de sign-on es deplegada.

Recomendaciones:

Esta pantalla informativa representa una herramienta que permite a los usuarios monitorear sus perfiles y detectar intentos de acceso no autorizados. Su uso es muy recomendable, sobre todo, entre usuarios con autoridades especiales y autoridades privadas sobre objetos críticos.

6.2.13 Intervalo de Expiración del Password (PWDEXPITV)

El cambio de passwords a distintos intervalos de tiempo reduce el riesgo de accesos no autorizados. Este campo controla el número de días que un password puede ser utilizado. Después de este límite, el sistema expira automáticamente el password al establecer el valor *YES en el campo PWDEXP. En consecuencia, el usuario requiere modificarlo durante su siguiente sign-on.

Valores Posibles:

- *SYSVAL — El valor del sistema QPWDEXPITV determina el intervalo de expiración para este usuario.
- *NOMAX — No se requiere que el usuario cambie su password.
- *Intervalo* — Un número en el rango de 1 a 366.

Recomendaciones:

- Establecer un intervalo de 60 días en QPWDEXPITV.
- Utilizar el campo PWDEXPITV para individuos que deben cambiar su password con mayor frecuencia.

6.2.14 Limitar Sesiones de Dispositivo (LMTDEVSSN)

Este campo controla la capacidad de sign-on's simultáneos del usuario en varias terminales. Este control no incluye la posibilidad de entablar una segunda sesión de trabajo en una misma terminal.

Valores Posibles:

- *SYSVAL — El valor indicado en la variable del sistema QLMTDEVSSN es utilizado.
- *NO — El usuario puede firmarse en varias terminales al mismo tiempo.
- *YES — El usuario no puede firmarse en varias terminales al mismo tiempo.

Recomendaciones:

- Definir el valor 1 en QLMTDEVSSN.
- Utilizar el campo LMTDEVSSN para aquellos usuarios que requieran firmarse en múltiples terminales.

6.2.15 Perfil de Grupo (GRPPRF)

El uso de este campo permite asociar al perfil de usuario con un perfil de grupo. La especificación del nombre del perfil de grupo convierte al usuario en miembro del grupo. El miembro hereda automáticamente todas las autoridades privadas que han sido asignadas al perfil grupal. Se requiere contar con las autoridades *OBJMGT y *CHANGE sobre el perfil de grupo para lograr esta relación.

Valores Posibles:

- *NONE — El perfil de usuario no se asocia a un perfil de grupo.
- *Nombre* — El nombre del perfil de grupo al que pertenece este perfil de usuario.

ESTA TESIS NO DEBE
SALIR DE LA BIBLIOTECA

Recomendaciones:

Esta característica de seguridad debe implantarse siempre que existan grupos de usuarios con necesidades de acceso a objetos muy similares.

6.2.16 Propietario (OWNER)

Este campo sólo puede ser utilizado cuando se ha especificado el nombre de un perfil de grupo en GRPPRF. Determina si el perfil de usuario individual o el perfil de grupo es el propietario de los objetos creados por el primero.

Valores Posibles:

- *USRPRF — Este perfil de usuario es el propietario de los objetos que crea.
- *GRPPRF — El perfil de grupo es el propietario de los objetos creados por el miembro y recibe la autoridad *ALL sobre todos ellos.

6.2.17 Autoridad del Grupo (GRPAUT)

Determina qué autoridades son transferidas del miembro al perfil de grupo cuando se ha especificado el valor *USRPRF en el campo OWNER. Estas autoridades se refieren a los objetos creados por el miembro.

Valores Posibles:

- *NONE — Ninguna autoridad específica es otorgada al perfil de grupo cuando este usuario crea objetos.
- *ALL — El perfil de grupo recibe todas las autoridades específicas sobre los objetos creados por este usuario.
- *CHANGE — El perfil de grupo puede modificar los objetos creados por este usuario.

- *USE — El perfil de grupo puede consultar los objetos creados por este usuario.
- *EXCLUDE — El perfil de grupo no puede accesar los objetos creados por este usuario.

6.2.18 Autoridad (AUT)

Este campo define la autoridad pública sobre el perfil de usuario.

Valores Posibles:

- *EXCLUDE — El público no tiene acceso al perfil de usuario.
- *ALL — El público cuenta con todas las autoridades específicas sobre el perfil de usuario.
- *CHANGE — El público puede modificar el perfil de usuario.
- *USE — El público puede consultar el perfil de usuario.

Recomendaciones:

La asignación del valor *EXCLUDE en todos los perfiles de usuario representa una medida adecuada para prevenir modificaciones no autorizadas a estos objetos.

Conclusiones

Conclusiones

Los procesos de identificación, autentificación y autorización que fundamentan el control de acceso lógico en los computadores modernos son de fácil comprensión y pueden resultar, hasta cierto punto, triviales. En la práctica, sin embargo, su implantación y administración constituyen actividades agotadoras y muy complejas. Son demasiados los detalles y conceptos que deben conocerse y asimilarse.

El AS/400 no es la excepción. Su arquitectura de seguridad es bastante complicada y demanda muchos meses de estudio y práctica. En algunos casos, es necesario cometer errores para entender plenamente su funcionamiento, ya que la literatura existente no es del todo clara en el tratamiento de ciertos aspectos.

El presente trabajo ha significado una labor extenuante de recopilación, análisis e interpretación de la información contenida en diversos manuales técnicos y libros. El material presentado incluye la explicación de las principales características y facilidades de control de acceso lógico presentes en el AS/400. Po lo tanto, puede facilitar la comprensión de su arquitectura de seguridad entre aquellos profesionales dedicados al control informático.

En mi opinion, dichas facilidades representan herramientas poderosas en la prevención de accesos no autorizados a los recursos almacenados en el sistema. No obstante, este potencial también puede llegar a ser confuso e, inclusive, degradar el desempeño del equipo cuando existen demasiados usuarios, objetos y autoridades específicas. Además, la asignación de autoridades especiales a ciertos individuos siempre descubre riesgos de control y vulnerabilidades importantes.

Históricamente, el control de acceso lógico siempre ha representado el lado obscuro de la Informática en muchas de las organizacions contemporáneas. Las justificaciones o pretextos que explican su relegamiento son muchos y muy pobres, desde una perspectiva de control.

Es justo reconocer que los fabricantes de hardware y software se han esforzado por dotar a sus productos de mejores opciones para restringir el acceso a la información. Desafortunadamente, en la actualidad estas mejoras se ven constantemente superadas por los frecuentes cambios en las tendencias tecnológicas que caracterizan a esta industria.

En el futuro, cuando la transición de una sociedad industrial a una sociedad basada en la información y el conocimiento se haya completado, todos proclamaremos la importancia de la seguridad y el control de acceso, pero pocos lograrán establecer ambientes de operación seguros. La proliferación masiva de grandes redes de comunicaciones entre computadores heterogéneos (interconectividad), el

establecimiento de filosofías abiertas de procesamiento y la adopción de arquitecturas cliente/servidor en las aplicaciones plantearán una descentralización absoluta de los aspectos relacionados con la seguridad. No existe en este momento la tecnología de control requerida para garantizar la integridad, confidencialidad y disponibilidad de la información en estos ambientes.

Sólo espero que la humanidad aprenda a controlar sus invenciones para no perecer.

Bibliografía

Bibliografía

IBM. (1988). IBM Application System/400 Technology.

IBM. (1990). Application System/400, System Operations; Operator's Guide. (3a. ed.).

IBM. (1990). AS/400 Security and Auditing Considerations, Release 2. International Technical Support Center. Poughkeepsie, NY.

IBM. (1992). Application System/400, Security Reference, Version 2. (2a. ed.).

IBM. (1992). IBM Application System/400 Technology Journal, Version 2.

IBM. (1992). Application System/400, System Concepts, Version 2. (2a. ed.).

IBM. (1992). Application System/400, System Introduction, Version 2. (2a. ed.).

IBM. (1993). IBM AS/400 System Handbook. (12a. ed.).

The Institute of Internal Auditors Research Foundation. (1991). Systems Auditability and Control Report, Module 9, Security. Altamonte Springs, FL.

The EDP Auditors Foundation. (1991). The EDPAA CISA Review Manual. Carol Stream, IL.

Price Waterhouse. (1988). Audit Guidance Series, Computerized Information Systems.

Price Waterhouse. (1992). System Management Methodology, Disaster Contingency Planning, Overview and Baseline.

Weber, Ron. (1988). EDP Auditing Conceptual Foundations and Practice. (2a. ed.). Mc Graw-Hill. Singapur.