Implementación de Estrategias y Directrices para la seguridad del AS/400

Creado por
Wayne O. Evans
AS/400 Security Consultant

E-mail: WOEvans@aol.com
Phone: (520) 578-7785

Este es un documento en proceso y está siendo distribuído para recibir comentarios. Tus comentarios serán bienvenidos apreciados. - Wayne O. Evans

Revisión Final.

Los sistemas AS/400 y la Aplicación de la Seguridad

Los sistemas AS/400 y la Aplicación de la Seguridad

Perspectiva general del Documento.

PROPÓSITO

El propósito de este documento es establecer una política de seguridad del AS/400 para {SU_EMPRESA} ({SUS_INICIALES}). Este documento le dará directrices en la implementación de estándares de seguridad que pueden ser utilizadas tanto por los desarrolladores de aplicaciones como por los responsables de seguridad.

Además de la seguridad del sistema, la protección de los datos depende de controles de la Dirección. Estos controles de los managers a menudo suponen una revisión de acciones por parte de personal independiente. Este documento se centra en la implementación en el AS/400 y en la recolección de datos para hacer posibles estas revisiones independientes pero sin el detalle de los procedimientos requeridos que aseguran su independencia.

APROBACIÓN

Este documento fue aprobado ___(fecha)_____ por _____(el aprobador)___.

Para desviaciones o cambios de este documento , contactar

Título
Dept xxxx

Este documento ha sido preparado por
Wayne O. Evans
5677 West Circle Z Street
Tucson, Arizona 85713-4416
WOEvans@aol.com
Phone (520) 578-7785

Los sistemas AS/400 y la Aplicación de la Seguridad

Objetivos del Control

Los estándares de control interno de {SU_EMPRESA} ({SUS_INICIALES}) han establecido los siguientes objetivos de control. El departamento de auditoría está encargado de hacer que se cumplan estos controles.

1. Salvaguardar los activos a través de la división de funciones y responsabilidades en la organización y la dirección de Recursos Humanos.

2. Asegurar que los nuevos sistemas coinciden con los requerimientos del usuario, son desarrollados acorde con las restricciones de presupuesto y tiempo, son mantenibles, contienen controles apropiados y las transacciones procesadas están documentadas.

3. Asegurar que las modificaciones de los sistemas operativos están autorizadas , controladas y testeadas , que la documentación relacionada está convenientemente actualizada y que se mantiene la integridad de los datos .

4. Asegurar que los registros en todos los sistemas están soportados por transacciones documentadas y encajan con los requisitos legales y de la Compañía {SU_EMPRESA}

5. Asegurar que la seguridad es adecuada para proteger las instalaciones , el equipamiento , el personal ,y los programas y ficheros de datos de posible destrucción o daño , bien accidental bien deliberada y para mantener la integridad de las operaciones de las computadoras. En caso de un evento así, minimizar la interrupción del negocio a través de una respuesta efectiva planificada.

6. Asegurar que los procesos están planificados, controlados y autorizados para utilizar efectivamente los recursos de procesos de datos y que encajan con los requerimientos de usuario.

7. Asegurar que el sistema y las bibliotecas de programas y los ficheros de datos están protegidos frente a accesos y modificaciones no autorizados.

Los sistemas AS/400 y la Aplicación de la Seguridad

Estrategia de Seguridad

Esta sección describe la estrategia de implantación de la seguridad basada en los objetivos de seguridad anteriores. Esta estrategia está desarrollada con recomendaciones en detalle.

Separación de Delegaciones.

Las operaciones de ({SUS_INICIALES}) están separadas en regiones geográficas llamadas DELEGACIONES . El mismo sistema de producción debe contener datos para múltiples delegaciones. Cada mercado debería estar separado para que así los usuarios de una delegación no dispongan de acceso a la otra delegación. Los datos de las delegaciones están separados en bibliotecas separadas del AS400 ,a las que sólo están autorizados los usuarios de esa delegación.
El acceso del usuario a los datos de la delegación debe ser determinado y aprobado por el Coordinador de Acceso de Delegaciones (MAC) o sus ayudantes.

Responsabilidad de los Usuarios

El acceso a los sistemas de ({SUS_INICIALES}) está limitado a personal autorizado. Los individuos a los que se ha concedido acceso a los sistemas de ({SUS_INICIALES}) son responsables del mantenimiento de la información confidencial de ({SUS_INICIALES}) y de no compartir sus contraseñas.Los usuarios del AS/400 serán identificados por un perfil de usuario individual y de esta forma, sus transacciones serán atribuídas a un único individuo. **(No está permitido el uso compartido de perfiles de usuario)**

División de Funciones

Las responsabilidades para los individuos deberían estructurarse de forma que un individuo no puede iniciar, aprobar , ejecutar o revisar ninguna transacción financiera. Los programas informáticos deben hacer cumplir esta división de obligaciones al no permitir a los usuarios el acceso más allá del alcance de las tareas que tiene asignadas.Igualmente, el equipo de programadores no está autorizado a modificar una aplicación y moverla a producción.

Separación de Programación y Producción

El equipo de programación tiene las enteras funciones de programar en máquinas de desarrollo. El desarrollo de programas (introducción de código, compilación y test) se hace en los sistemas de desarrollo. Cuando los programas se han completado, se moverán a máquinas de prueba. En estas máquinas de test, los programadores pueden probar esos programas pero todas las compilaciones deben hacerse en las máquinas de desarrollo.

La implementación y cambios en las aplicaciones informáticas (programas) debe realizarse en entorno separado de los datos de producción. Los programas que hayan sido testeados se moverán a producción bajo el control de coordinadores de los cambios.

Los sistemas AS/400 y la Aplicación de la Seguridad

Auditoría

El diseño de las aplicaciones debe soportar el “logging” de las transacciones de usuario. Las aplicaciones y los registros de auditoría del sistema incluirán el nombre de ese perfil de usuario que realiza la transacción.
Las acciones de usuarios con acceso que permite el acceso sin restricciones (autorizacoines especiales como *ALLOBJ, *SPLCTL) quedará registrado en el journal de auditoría del sistema. En caso de que en el staff de programadores se disponga de accesos potentes para resolver emergencias, las acciones de esos usuarios serán registradas en el journal de auditoría y revisadas por terceras partes independientes.

Los sistemas AS/400 y la Aplicación de la Seguridad

Perspectiva general de la Seguridad.

Estructura de los perfiles de usuario y grupo.

La Figura 1 Estructura de los perfiles de Usuario y los Programas de Inicio en la página 7 ilustra la interacción de los perfiles de usuario y grupo y el programa de Inicio. Los siguientes aspectos explican detalles de la figura.

❶ Los perfiles de Grupo se usan para simplificar la gestión de la seguridad. El acceso a objetos se concede a perfiles de grupo en vez de a usuarios con perfiles individuales. Se definirán distintos perfiles de grupo para cada delegación.

Si la delegación tiene múltiples aplicaciones que necesitan de diferente seguridad, la delegación tendrá un propietario y perfil de grupo para cada aplicación de forma separada. Esto está ilustrado en el ejemplo ❻ en la Figura 3 de la pág. 9.

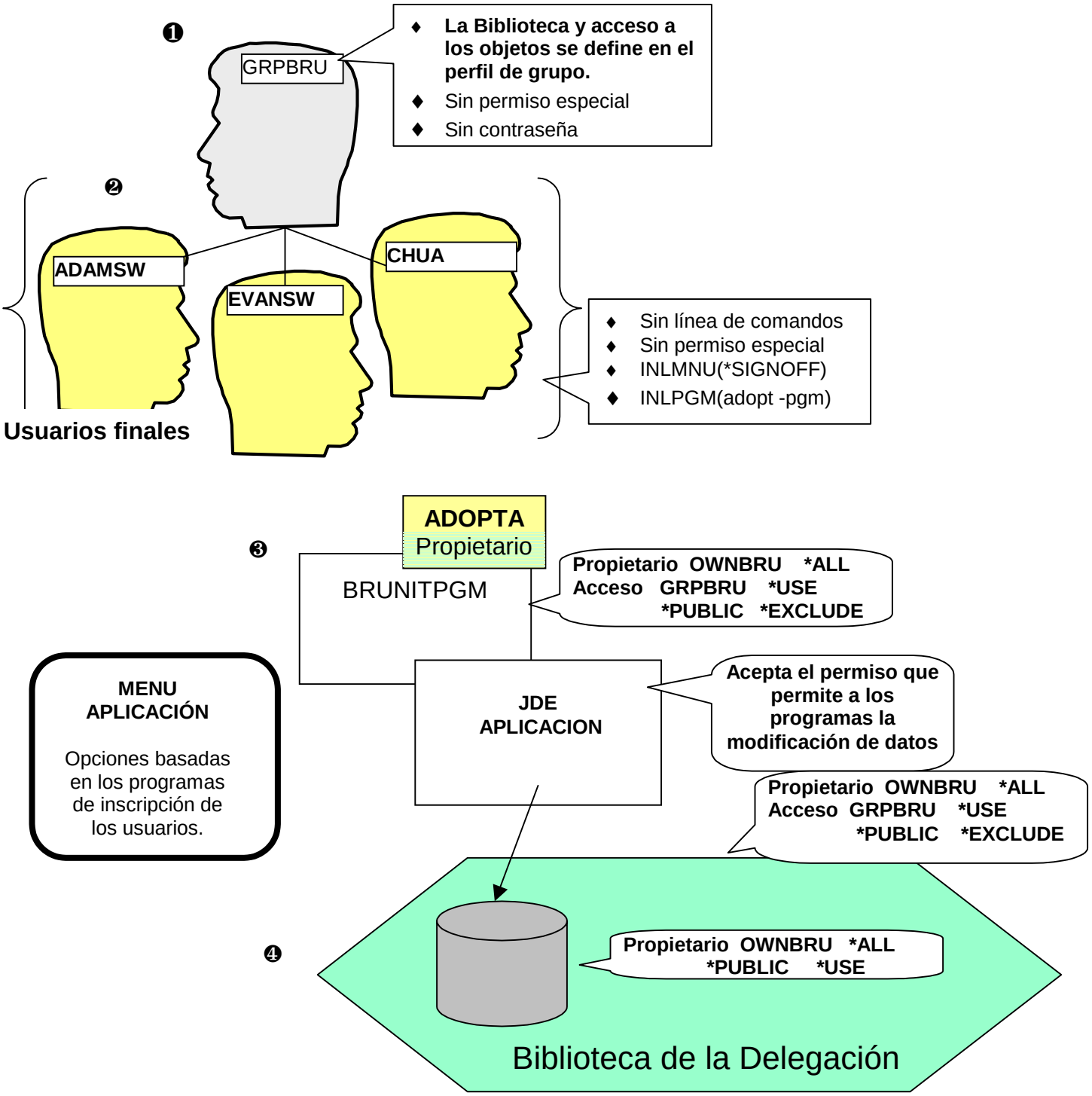
❷ Los perfiles de usuario individuales se definen para usuarios finales. Los usuarios finales no tienen acceso a la línea de comandos y funciones de los programas limitadas . Su perfil de grupo y el programa de Inicio determinan el acceso de los individuos a los datos .

❸ El programa de Inicio adopta el permiso del propietario de los datos de la delegación. Basado en la inscripción de la aplicación (el nivel de seguridad de las aplicaciones), los programas muestran los menus con las opciones apropiadas para dar a los usuarios el acceso a los datos. Este permiso permite a los programas interactivos actualizar los datos de producción.

❹ Los usuarios están autorizados a crear programas a medida para analizar los datos usando aplicaciones de PC y el query. El permiso público a los datos de producción es *USE ,el cual permite a los usuarios la descarga (pero no la carga) de datos desde el AS/400 a un PC. Únicamente los usuarios autorizados de esa biblioteca son miembros de la delegación a la que pertenecen los datos. Esto previene el acceso a los datos de la delegación por usuarios externos a dicha delegación.

Los sistemas AS/400 y la Aplicación de la Seguridad

Figura 2 Estructura de los perfiles de Usuario y los Programas de Inicio



Los sistemas AS/400 y la Aplicación de la Seguridad

Separación de delegaciones

La seguridad del AS/400 evita que los usuarios de una delegación accedan a los datos de otra delegación incluso aunque esas distintas delegaciones estén presentes en la misma máquina.Esto está ilustrado en la Figura 3 Separación de Delegaciones de la página 10 .El siguiente texto describe esa figura.

❶ Cada delegación está representada por múltiples bibliotecas de AS/400. A efectos de backup las bibliotecas están divididas en ejecutables y bibliotecas de datos.

❷ Los perfiles de grupo que representan esa delegación están autorizados en las bibliotecas de la delegación . Otros usuarios que no están autorizados a esas bibliotecas de la delegación no tendrán acceso a los ficheros de datos de la delegación.

❸ El permiso *PUBLIC para los datos es *USE , así los usuarios dentro de la delegación están autorizados a copiar los datos de la delegación a efectos de crear informes. Los usuarios podrán descargar los datos a sus PCs para realizar un análisis con hojas de cálculo y usar los query del AS/400.

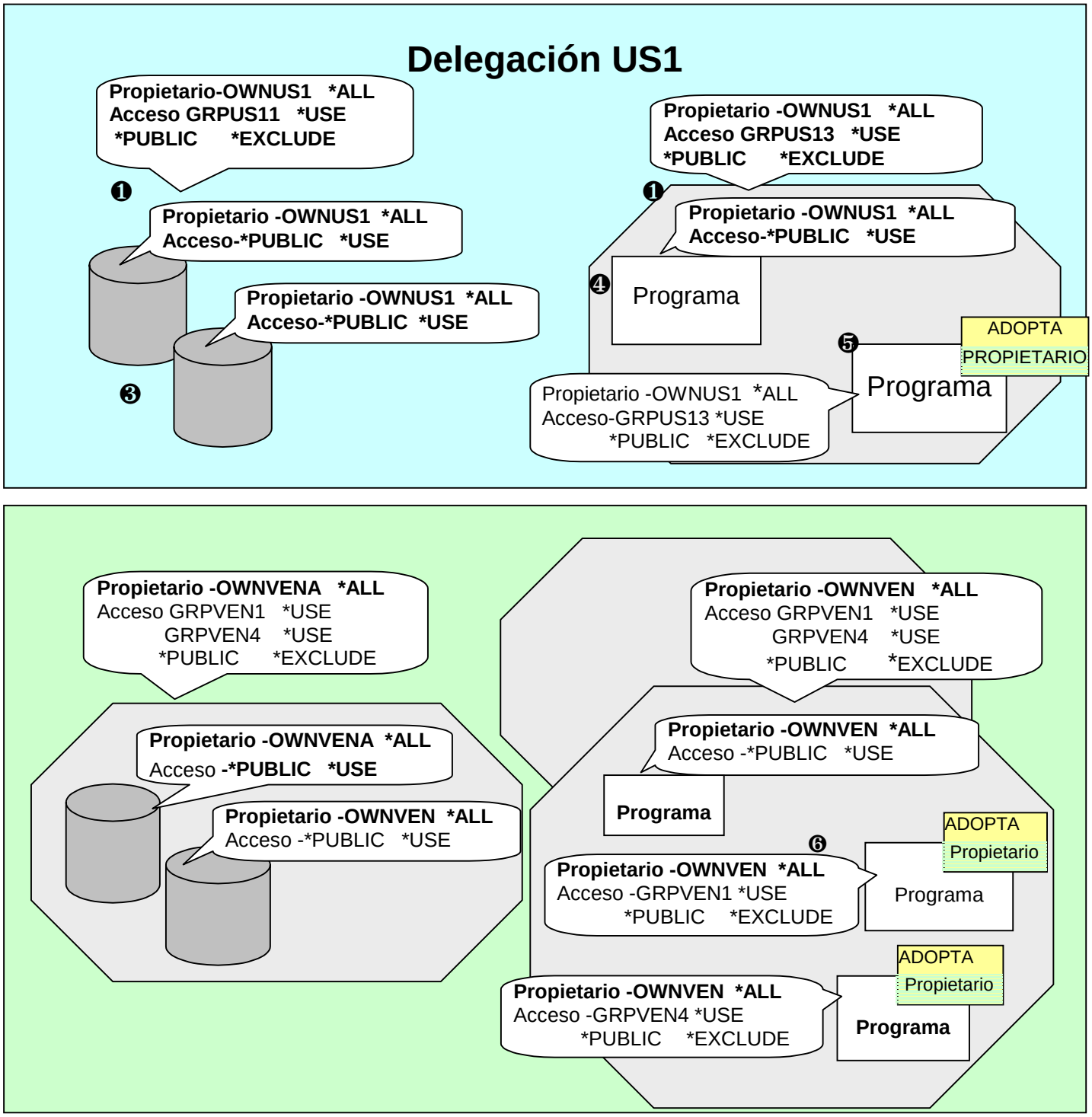
❹ El programa que se muestra representa una modificación local de la aplicación base que se aplica sólo para esta delegación.

❺ La biblioteca del ejecutable contiene los programas de producción y el programa de inicio para los usuarios de la delegación. El programa de inicio acepta el perfil como el propietario de los datos de la delegación y así el usuario puede actualizar los ficheros de datos cuando utiliza los programas. El programa de Inicio se usará para personalizar las opciones de menú de los usuarios. Todos los usuarios con las mismas opciones de menú (nivel de acceso a los programas) tendrán su propio programa inicio.

❻ En un entorno de seguridad complicada, deberán existir múltiples programas de Inicio para la misma delegación . Este puede ser el caso cuando múltiples programas dentro de la misma delegación requieren de seguridad por separado. Por ejemplo , los programas de Recursos Humanos necesitan distinta seguridad que la información de las ventas.

Los usuarios serán autorizados al programa de inicio que les corresponda según su nivel de acceso a los programas. Restringir el acceso al programa de Inicio evita que los usuarios que dispongan de acceso a la línea de comandos puedan realizar llamadas directamente al programa de Inicio. *Este diseño está recomendado incluso cuando no existe la intención de otorgar a los usuarios acceso a la línea de comandos, porque el equipo de programadores tendrá acceso a la línea de comandos para situaciones que necesitan alguna reparación. Si estas decisiones debieran retrocederse en el futuro, los programas de Inicio estarán seguros.*

Figura 3 Separación de Delegaciones



Los sistemas AS/400 y la Aplicación de la Seguridad

Adopción en Batch

El programa de Inicio de los usuarios acepta la autorización y lo propaga para llamar a los programas interactivos. Este permiso adoptado permite a los programas actualizar los ficheros de datos. Cuando un programa interactivo somete una petición de batch, el permiso adoptado desde el trabajo interactivo no se propaga al trabajo batch .

Los trabajos batch necesitan también de un permiso para actualizar los datos de producción. La Figura 4 Adopción en Batch ilustra los pasos en la ejecución de los trabajos batch. A la derecha está la versión modificada que utiliza un programa shell para la adopción de permisos antes de iniciar el programa.
. El texto siguiente describe la figura .

❶ El programa de inicio en los trabajos interactivos adopta el permiso y propaga esos permisos adoptados en los programas llamados. Esto permite a los programas acceder a los datos de producción del mercado.

Los programas interactivos deben someter trabajos batch (SBMJOB) para procesar las peticiones del usuario. La petición se convierte en un trabajo batch que se almacena en la cola de trabajos batch y queda planificada para su ejecución.

❷ Si el trabajo batch fuera procesado por el subsistema estándar de batch, el programa que suministra IBM ,QCMD, iniciaría la aplicación sin permisos atribuídos. Como el programa no dispone de permisos para actualizar los ficheros de producción, las peticiones de modificar los datos de producción serán rechazadas.

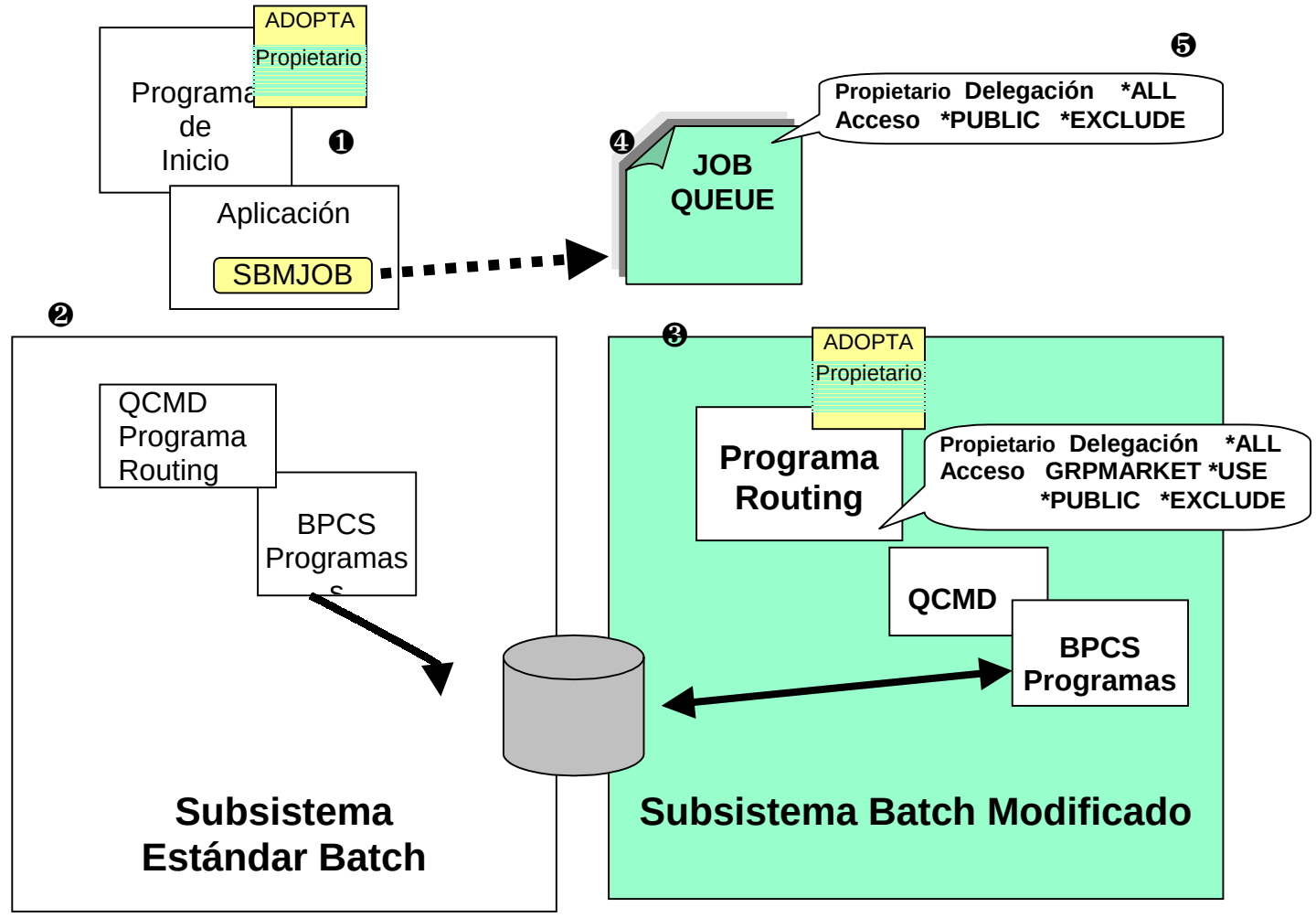
❸ El subsistema modificado tiene una programa shell de enrutamiento que asume como el propietario de los datos de la delegación. Este permiso asumido se propagará a la aplicación BPCS para su ejecución.Este permiso autoriza al programa para modificar los datos de producción.

❹ Cada delegación tendrá una JOBQ y un subsistema batch que procesará los trabajos sólo de esa delegación.Los subsistemas tendrán un programa de enroutamiento diferente que será asumido por el propietario de los datos de esa delegación .

❺ Puesto que los trabajos sometidos a la JOBQ se ejecutan con el permiso adoptado, el permiso a JOBQ deberá restringirse de forma que únicamente se aceptaran trabajos sometidos desde la sesión interactiva.

NOTA: Los operadores del sistema no tendrán acceso a esta JOBQ a menos que ejecuten un programa que les conceda acceso.

Figura 4 Adopción en Batch



Los sistemas AS/400 y la Aplicación de la Seguridad

Detalles de la Seguridad del AS/400.

Esta sección del documento ofrece líneas de trabajo para implementar las políticas de seguridad. El enfoque del documento está en el entorno de la producción, no de los sistemas utilizados para desarrollar o pruebas.

Los usuarios serán uno de estos tipos :

1. Usuarios finales de la Delegación (USER)—Los usuarios finales no tienen acceso a la línea de comandos. Los menus de programas incluirán opciones para ver y manejar el output impreso. Los usuarios finales pueden tener algún acceso a herramientas más poderosas como la descarga de ficheros o la obtención de informes.

2. Coordinadores del Acceso a las Delegaciones (MAC)---Usuario final con opciones especiales para comunicarse con la Administración de la Seguridad para la gestión de los usuarios y sus accesos. Revisa y realiza el seguimiento de las violaciones de acceso (reportadas) a los datos de la delegación . El journal de auditoría del AS/400 puede usarse para recopilar estas violaciones de los accesos. La inscripción a las aplicaciones la realizará este Coordinador.

3. Administradores de la Seguridad (SA)---Usuarios responsables de llevar a cabo las tareas de creación de usuarios y la designación de sus accesos. Todos los comandos y cambios en la seguridad que realicen estos usuarios se grabarán en el journal de auditoría.
   Las actuales prácticas empresariales de ({SUS_INICIALES}) utilizan una gestión de la seguridad centralizada .Esta práctica puede reemplazarse por la inscripción / eliminación de los usuarios descentralizada,creando programas que los coordinadores de acceso usarán pra dar de alta o de baja a los usuarios finales.

4. Administradores de Help Desk ---Usuarios con conocimientos básicos con acceso a opciones de menú para eliminar contraseñas olvidadas y ayudar a los usuarios finales en problemas relacionados con los programas. Estos usuarios no disponen de acceso a la línea de comandos y tendrán opciones de menú que les habilitan el acceso necesario.

5. Operadores de Sistema ---Usuarios con acceso a línea de comandos y permisos especiales para *JOBCTL y *SAVSYS . Estos usuarios pueden realizar un backup del sistema y someter trabajos de producción a batch.

6. Administradores de la Red ---Usuarios con acceso a línea de comandos y permisos especiales para *IOSYSCFG y *JOBCTL y tienen la responsabilidad de la definición y mantenimiento de las configuraciones de las comunicaciones. Estos usuarios no tendrán permisos especiales *ALLOBJ

7. Programadores de Aplicaciones--- Los programadores dispondrán de plenas capacidades en las máquinas de desarrollo. En las máquinas de test ,los programadores tendrán acceso a la línea de comandos pero estarán restringidos a sólo lectura para los ficheros de producción cuando no ejecuten los programas. No estarán autorizados para usar las utilidades de modificación de datos

para corregir datos de los ficheros.

8. Administradores de la Gestión de los Cambios ---Usuarios que controlan los cambios con acceso a modificar objetos de producción como parte de un cambio autorizado.

9. Responsable de la Seguridad del Sistema (QSECOFR)---Este no se utiliza excepto en caso de emergencia (recuperación de algún desastre) o instalación de una nueva versión. Todos los comandos introducidos serán registrados en el journal de auditoría.

10. Ingenieros del Sistema —Usuarios con acceso a la línea de comandos y la responsabilidad de crear e instalar la configuración de subsistemas y programas de utilidades.

Otros perfiles de usuario no utilizados para sign-on (Contraseña *NONE)

1. Perfiles de IBM y Software ---Estos perfiles no se utilizan en ejecución normal. El perfil habilita a los propietarios del software para controlar cambios o herramientas de auditoría.
2. Perfiles de Propietario de Objetos.---El propietario de datos de producción y objetos ejecutables. Este perfil lo asume el programa de Inicio para los usuarios finales y no dispone de permisos especiales.
3. Perfiles de Propietario Especial ---Estos perfiles tendrán permisos especiales (*SECADM, *JOBCTL, *SAVSYS) como los requeridos para el borrado de contraseñas , acceso especial a producción, etc.
4. Perfiles de Grupo---Utilizado para simplificar la gestión de la seguridad , los perfiles de grupo tendrán acceso a los trabajos y colas de output , programas de producción y bibliotecas de la delegación.

Atributos del perfil de Usuario y Grupo

Los atributos del perfil de usuario en sistemas de producción se muestra en la Tabla Tabla 1 Atributos del perfil de Usuario . Los nombres del perfil de usuario individual deberían limitarse a 8 caracteres, de forma que el identificador de usuario de la Red (el que utiliza SNADS y Lotus Notes) puede ser el mismo que el perfil de usuario. La estructura de los nombres del perfil de usuario será LLLLLFnn donde

LLLLL	Apellido (maximo 5 caracteres)
F	Primera inicial (maximo 1 carácter)
nn	(Opcional) 2 dígitos que se usan para resolver posibles duplicados.

Tabla 1 Atributos del perfil de Usuario y Grupo

Perfiles de Grupo						
	Usuarios finales	Admin Seguridad	Operadores Sistema	Help Desk	Admin Red	Ingenieros Sistema
Nombre Perfil	GRPXXYUSR	GRPSECADM	GRPSYSOPR	GRPHELP	GRPNETADM	GRPSYSENG
USRCLS	*USER	*SECOFR	*SYSOPR	*SYSOPR	*PGMR	*PGMR
SPCAUT	*NONE	*ALLOBJ SECADM	*JOBCTL *SAVSYS	*JOBCTL	*IOSYSCFG* JOBCTL *SERVICE	IOSYSCFG* JOBCTL *SERVICE
PASSWORD	*NONE	*NONE	*NONE	*NONE	*NONE	*NONE

Tabla 2 Atributos del perfil User y los miembros de Grupos.

	Usuarios finales	Admin Seguridad	Operadores Sistema	Help Desk	Admin Red	Ingenieros Sistema
LMTCPB	*YES	*NO	*NO	*YES	*NO	*NO
USRCLS	*USER	*SECOFR	*SYSOPR	*PGMR	*PGMR	*PGMR
INLPGM	A determinar	*NONE	*NONE	A determinar	*NONE	*NONE
INLMNU	*SIGNOFF	MAIN	MAIN	MAIN	MAIN	MAIN
GRPPRF	GRPXXYUSR	GRPSECADM	GRPSYSOPR	GRPHELP	GRPNETADM	GRPSYSENG
OWNER	*GRPPRF	*GRPPRF	*GRPPRF	*GRPPRF	*GRPPRF	*GRPPRF
CURLIB	xxyaaaaPF	{YOUR_INITIALS}SEC	{YOUR_INITIALS}GPL	{YOUR_INITIALS}GPL	{YOUR_INITIALS}GPL	{YOUR_INITIALS}GPL
PWDEXP	*YES[1]	*YES[1]	*YES[1]	*YES[1]	*YES[1]	*YES[1]
PWDEXPITV	*SYSVAL	*SYSVAL	*SYSVAL	*SYSVAL	*SYSVAL	*SYSVAL
ATTNPGM	xxyCOMUTIL	{YOUR_INITIALS}COMUTIL	{YOUR_INITIALS}COMUTL	HLP{YOUR_INITIALS}UTL	{YOUR_INITIALS}COMUTL	{YOUR_INITIALS}COMUTL
ACGDTA	xxyaaaadddd[2]	xxyaaaadddd[2]	xxyaaaadddd[2]	xxyaaaadddd[2]	Xxyaaaadddd[2]	xxyaaaadddd[2]

Nota 1: La contraseña se configurará para caducar para los perfiles nuevos y así requerirá a los usuarios el cambio de contraseñas en su primer sign-on

Note 2: El “accounting field “ del usuario se usará para asignar usuarios a los recursos de la computadora. El campo será xxy = designación delegación aaaa = aplicación y dddd = designación departamento.

El acceso de los programadores variará según el entorno del sistema, la Figura 5 ilustra el acceso del programador en diferentes entornos.

Figura 5 Acceso Programadores en Distintos Entornos.

	Desarrollo	**Test**	**Producción**
USRCLS	*PGMR	*PGMR	
Línea Comandos	Si	Si	No
Permisos especiales	*JOBCTL	*NONE	*NONE
Consideraciones especiales del entorno	Verificar fuentes de bibliotecas privadas.		Si es necesario los comandos para debug pueden cambiarse para permitir la resolución de problemas en las aplicaciones.
Permite la compilación de programas.	SI	NO	NO

Cada delegación identificará a un Coordinador de Acceso a la Delegación (MAC) que tendrá la responsabilidad de designar los usuarios y el nivel de acceso que se les permite en la delegación. El MAC debería designar un mínimo de asistentes de backup . Los nombre del MAC y sus asistentes deberá comunicarse a los administradores de seguridad.

Las responsabilidades del MAC incluyen:

1. Notificar a la Administración de la Seguridad las nuevas altas y bajas de usuarios.
2. Notificar los nuevos o cambios en los niveles de acceso de los usuarios.
3. Revisiones periódicas y aprobación de todos los usuarios y su nivel de acceso a los datos de la delegación .
4. Revisión y seguimiento de las violaciones de acceso reportadas.
5. Ser un recurso para la política de seguridad , incluyendo la definición de un modelo de acceso y trabajar con los Responsables de Seguridad en la definición de aquellos datos delicados que requieren de una protección especial.

Las responsabilidades de los Administradores de Seguridad (SA) incluyen:

1. Definición y monitorización de los controles globales.
   - valores de sistema,
   - programas de salida (exit programs) para controlar el acceso de los usuarios (DDMACC, PCSACC, FTP, Perfil de Usuario)
   - Listas de permisos especiales QPWSERVER y QUSEADPAUT.
     Ver apéndice (A-C) de este documento para consultar los valores recomendados del sistema , atributos de red y ejemplos de programas de salida
2. Altas/ Bajas de usuario incluyendo el sistema y los procedimientos de las aplicaciones de alta.
3. Creación y mantenimiento de los permisos para los objetos y listas de permisos.
4. Monitorización de perfiles sin usar y usuarios rescindidos.
5. Ejecutar y monitorizar los informes de auditoría y los informes de gestión de la seguridad.
6. Definición de los requisitos de backup y restauración para los usuarios y datos.
7. Identificación de las herramientas para help desk y para las tareas de gestión de la seguridad.
8. Ayudar al help desk y al equipo de programación en la solución de problemas en la aplicación de la seguridad.
9. Ayudar en la definición de un modelo de seguridad para el control de cambios.
10. Monitorización de la propiedad de objetos
    - El perfil de usuario QDFTOWN no debe poseer ningún objeto.

- La transferencia de la propiedad de objetos[1] creados dinámicamente por usuarios a perfiles OWNXXY .

(Esta operación puede no ser necesaria si la aplicación transfiere la propiedad)

[1] Si una aplicación crea ficheros u otros objetos, los ficheros serán propiedad del perfil de grupo de usuario final GRPXXY en vez de el perfil de propietario de objetos OWNXXY.

Los sistemas AS/400 y la Aplicación de la Seguridad

Supuestos a verificar

Esta sección se usa para comunicar las supuestos que necesitan ser verificados.

1. El acceso sólo de lectura a los ficheros de datos se permite a los usuarios de la delegación pero se evita la modificación fuera de los programas.

2. Esto está controlado por el permiso *PUBLIC en los ficheros, y podría ser más restrictivo pero creará problemas para la descarga de ficheros y las aplicaciones de query.

3. Existen en la actualidad programas cliente –servidor de AS/400 que actualizan los datos de producción.

El permiso *PUBLIC para los ficheros permite el acceso para lectura a través de programas PC usando ODBC pero no modifica operaciones. Varias alternativas de implantación se discuten en el Apéndice D : Consideraciones de Seguridad del Acceso ODBC.

DEBERA SELECCIONARSE UNA DE ESAS ALTERNATIVAS.

Los sistemas AS/400 y la Aplicación de la Seguridad

Consideraciones sobre los programas

Esta sección se usa para comunicar las consideraciones de seguridad para el desarrollo de aplicaciones .

1. Los menus de las aplicaciones tendrán opciones que permitan a los usuarios la gestión y visualización de sus propios ficheros de spool y los trabajos sometidos sin que para ello deban depender de la introducción de comandos OS/400.

2. Los controles de seguridad del programa determinan qué opciones del menú y qué operaciones pueden realizar usuarios individuales mientras usan la aplicación. Esta información del nivel de seguridad del programa será referida en este documento como la aplicación para inscribir o dar de alta. La información del programa de altas se archiva normalmente en una base de datos de ficheros organizada por usuario. Donde sea posible, esta información del programa de altas deberá centralizarse en ficheros de alta comunes. Esto permitirá a la auditoría ver el acceso de los usuarios en una determinada ubicación.

   Una técnica para un intruso para ganar acceso adicional es la creación de una versión alternativa de los ficheros del programa de altas. Suministrando un comando (OVRDBF) previo a la llamada del menu del programa , un intruso (hacker) podría posiblemente expandir su acceso. PARA PREVENIR el redireccionamiento (override) de los ficheros de altas, el programa de Inicio para batch e interactivos debe suministrar un comando override con la opción SECURE(*YES) option.
   OVRDBF FILE(fichero de altas) SECURE(*YES)

3. Los programas deberían ser implementados utilizando interfaces OS/400 . Los interfaces de S/36 y S/38 no estarán disponibles en sistemas de desarrollo o producción.

4. Esto eliminará la necesidad de asegurar los comandos en la biblioteca QSYS38 así como los comandos en la biblioteca QSYS. Este es un descuido de seguridad muy frecuente.

5. El programa de Inicio para usuarios interactivos tendrá acceso a los datos de producción. Cualquier programa que muestre una línea de comandos debe especificar USEADPAUT(*NO) para evitar el acceso de los usuarios a los comandos con el acceso adoptado. Mientras la mayoría de usuarios no tendrán la línea de comandos, los programas deben diseñarse para acomodarse a la posibilidad de que algunos usuarios tengan acceso a la línea de comandos en su perfil de usuario.

   NOTA: Una aplicación que soporta el acceso a la línea de comandos vía tecla de atención no es un riesgo. Los programas de tecla Atención no toman los permisos adoptados.

6. Los programas estarán definidos para añadir o quitar a los usuarios de la aplicación en los ficheros de control del programa. Los programas de baja deberían poder ser llamados como programas de salida desde DLTUSRPRF (borrar perfil de usuario), pasando el nombre del usuario de ese perfil y toda la información del programa de altas.

   Fallar en la limpieza de los ficheros del programa de altas es un riesgo potencial de que un usuario sea borrado y entonces el mismo nombre de perfil de usuario lo utilice un nuevo usuario. El nuevo usuario debe conseguir el alta del usuario anterior.

7. Los programas deben prever los requerimientos de las transacciones de auditoría.

   Más detalles sobre los requisitos serán añadidos por el departamento de auditoría

8. En general, los programadores tendrán sólo acceso de lectura (read-only) a los datos de producción. En caso de una emergencia, se les dará acceso temporal a un programa (LOGCMD) que adquiere acceso propietario a los ficheros de los datos de producción. Mientres operen con el acceso de emergencia, todos los comandos (y cambios en los ficheros) se grabarán en los log de auditoría.

9. La implementación de la seguridad depende de los ficheros que son usados por el programa en propiedad del perfil de propietario de la delegación OWNXXY. Si un programa crea ficheros (otros distintos de ficheros temporales) que se utilizan fuera del trabajo creado, el propietario de estos nuevos ficheros creados deberá cambiarse por el perfil de propietario de la delegación OWNXXY e vez de el usuario individual o el grupo de usuarios individuales.

   La propiedad de los ficheros del propietario de la delegación en vez de la de su creador o del perfil de grupo evita que los usuarios tengan acceso a los datos que les permitirían modificar y borrar operaciones desde fuera del programa.

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Tabla 3 Valores de Sistema relativos a la Seguridad

Nombre	Valor Recomendado	Comentarios
QALWUSRDMN	*ALL	Permite Dominio de Usuario – Indica que todas las bibliotecas del sistema deben contener objetos de dominio del usuario (*USRSPC, *USRIDX, y *USRQ).
QALWOBJRST	*ALL	Permite Restauración Objetos –Determina si los objetos especialmente delicados en términos de seguridad pueden ser restaurados en el sistema. Puede usarlo para evitar que alguien restaure un objeto de estado del sistema o un objeto que adopta autorizaciones.
QATNPGM	*ASSIST	Programa de Ayuda – El Menu del Asistente de Operaciones aparece cuando se presiona la tecla de Ayuda.Puede estar omitido en el perfil de usuario .
QAUDCTL	*AUDLVL	Control de Auditoría- Indica que el sistema auditará según los objetos designados por el comando CHGOBJAUD y por el valor de sistema QAUDLVL.
QAUDENDACN	*NOTIFY	Acción de Fin de Auditoría – El operador del sistema será notificado cuando el journal de auditoría no pueda recibir más registros.
QAUDFRCLVL	*SYS	Nivel de frecuencia de la Auditoría – El sistema determinará cuando las entradas del journal serán escritas desde el journal de seguridad a los ficheros auxiliares.

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Nombre	Valor Recomendado	Comentarios
QAUDLVL	**Minimo** *AUTFAIL *SERVICE *SECURITY *SAVRST Opcional ***CREATE *DELETE *NETCMN *OBJMGT *OPTICAL *OFCSRV *PGMFAIL *JOBDTA *PRTDTA *SPLFDTA *SYSMGT **Evitar** *PGMADP	Nivel de Auditoría – El sistema grabará las acciones de los usuarios. La configuración mínima audita errores en la autentificación, la creación de objetos optativos, el borrado de objetos, el renombrar o mover objetos, funciones relativas a la seguridad (cambiar valores de sistema , cambios en los perfiles de usuario , derechos de acceso a los objetos , etc.), y violaciones del nivel 40 . Evitar : por razones de rendimiento ,la auditoría global de “program adopt “.
QAUTOCFG	1 (on)	AutoConfiguración – Esto se configura como off (0) durante las operaciones normales. Puede activarse como (1) para configurar automáticamente nuevos dispositivos, pero debe devolverse a off una vez el proceso se ha completado.
QAUTOVRT	300	Auto Virtual – Este valor representa el número máximo de dispositivos virtuales que se pueden configurar. El valor 0 “off” no evita la configuración Client Access/400 de los dispositivos virtuales.
QCRTAUT	*USE	Permiso público por defecto – El permiso público por defecto para los objetos creados. **NOTA**: El CRTAUT para la biblioteca QSYS debe configurarse como *CHANGE para que las descripciones de los dispositivos configurados automáticamente tengan el acceso adecuado para que los usuarios puedan sign-on
QCRTOBJAUD	*NONE	Crear Auditoría de Objetos – Establece la auditoría de objetos por defecto cuando son creados..

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Nombre	Valor Recomendado	Comentarios
QDEVRCYACN	**Preferido** *DSCENDRQS *ENDJOB *ENDJOBNOLIST **Opcional** *DSCMSG	Acción para la Restauración de Dispositivos – Acción del sistema cuando se reestablecen las comunicaciones, *DSCMSG Desconecta el trabajo. Cuando signing-on de nuevo , se envía un mensaje de error al programa del usuario. *MSG Señala el mensaje de error I/O en el programa de usuario . El programa ejecuta la recuperación de errores. *DSCENDRQS Desconecta el trabajo. Cuando signing-on de nuevo, actúa una función de petición de cancelación para devolver el control del trabajo de nuevo al último nivel de petición. *ENDJOB Finaliza el trabajo. Se produce un log para el trabajo. Un mensaje indica que el trabajo ha finalizado porque el error del dispositivo se envió al log del trabajo y al log QHST. *ENDJOBNOLIST Finaliza el trabajo.No se produce un log de trabajo .Un mensaje indica que el trabajo finalizó porque el error del dispositivo se envió al log QHST.
QDSCJOBITV	120	Intervalo para desconexión de Trabajos Time-out - Período de tiempo que transcurre antes que el sistema actúe sobre un trabajo desconectado.
QDSPSGNINF	1 (on)	Información en Pantalla Sign-on - El sistema mostrará una pantalla adicional en sign-on que contiene la fecha y hora de la última conexión y el número de intentos de sig-on no válidos.
QINACTITV	90	Intervalo de Inactividad - Los trabajos inactivos time out después de 90 minutos. En OS/400V4R2, TELNET y WSG miran ambos al valor de sistema QINACTITV .Para controlar las conexiones TELNET y WSG en releases anteriores, debe usar el parámetro INACTTIMO del comando Change Telnet (o WSG) Attributes .
QINACTMSGQ	*DSCJOB	Cola de Mensajes Inactivos -La acción que se ha tomado con los trabajos interactivos que dan time out

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Nombre	Valor Recomendado	Comentarios
QLMTDEVSSN	1 (on)	Limitar Sesiones de Dispositivo- Está limitado el número de dispositivos concurrentes en los que los usuarios se han autentificado.
QLMTSECOFR	1 (on) Durante desarrollo 0 (off)	Limita Security Officer – Usuarios con *ALLOBJ y permiso especial *SERVICE no pueden autentificarse en cualquier dispositivo configurado del sistema. La mayoría de usuarios incluso los administradores de seguridad no tendrán permiso *ALLOBJ en sus perfiles de usuario . Se les permitirá adoptar acceso *ALLOBJ cuando lo necesiten al usar LOGCMD.
QMAXSIGN	3	Intentos máximos de Sign-on – El número de intentos no válidos de sign-on que está permitido antes de que el perfil de usuario se desactive. Una vez que se ha realizado un sign-on con éxito , el contador vuelve a cero (0).
QMAXSGNACN	2	Intentos máximos de acciones Sign-on para prevenir más intentos ,una vez que el usuario alcanza el número máximo de intentos no válidos de sign-on 1. Deshabilita el dispositivo 2. Deshabilita el perfil de usuario 3. Deshabilita ambos, el dispositivo y el usuario
QRMTSIGN	*FRCSIGNON	Sign-on Remoto – Está permitido el sign-on remoto, pero el usuario debe sign-on con un perfil de usuario y passwords válidos. *FRCSIGNON Las peticiones de sign-on remoto deben atravesar el proceso sign-on. *SAMEPRF Cuando el nombre del perfil de usuario de origen y destino son el mismo , la pantalla de sign-on se evitará. *VERIFY El valor *VERIFY te permite evitar la pantalla de sistema sign-on en destino. *REJECT No se permite sign- on remoto

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Nombre	Valor Recomendado	Comentarios
QRETSVRSEC	0 (off)	Retener seguridad del servidor.Determina si los datos de seguridad que necesita un servidor para autentificar un usuario en el sistema destino a través del interface cliente-servidor pueden retenerse en el sistema servidor. Los valores que se aceptan son : 0 (off) Datos de seguridad del servidor no se retienen. 1 (on) Datos de seguridad del servidor se retienen.
QRMTSRVATR	0 (off)	El atributo Servicio Remoto controla el análisis del problema de servicio remoto. Valores aceptados son : 0 (off) Atributo del servicio remoto off. 1 (on) Atributo del servicio remoto on.
QSECURITY	**Preferido** 40	Nivel de seguridad -. El sistema requiere una contraseña para sign-on y los usuarios deben tener permisos para acceder a objetos y recursos del sistema. El Nivel 40 protege frente a la sumisión de trabajos utilizando JOBDs con nombre de usuario.

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Nombre	Valor Recomendado	Comentarios
QUSEADPAUT	*NONE	Usar Permiso Adoptado – define qué usuarios pueden crear programas con el atributo USEADPAUT(*YES) *NONE – Todos los usuarios autorizados pueden crear o cambiar programas y servicios de programa para usar el permiso adoptado si el usuario tiene el permiso necesario para el programa o servicios de programa. Lista de Autorizaciones . El valor de sistema puede contener el nombre de una lista de autorizaciones. La autorización del usuario se comprueba contra esta lista. Si el usuario tiene al menos permiso *USE en la lista de autorizaciones mencionada , el usuario puede crear, cambiar o actualizar programas o servicios de programa con el atributo USEADPAUT(*YES) . Para prevenir que cualquiera pueda crear programas que utilicen los permisos adoptados en las máquinas de producción, crear una lista de permisos con autorización *PUBLIC(*EXCLUDE). Especificar esta lista de permisos para el valor de sistema QUSEADPAUT.

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Tabla 4 Valores de sistema para Contraseña

Nombre	Valor Recomendado	Comentarios
QPWDEXPITV	90	Intervalo para Caducidad Contraseña – Las contraseñas se configuran para caducar cada nn días. Los usuarios se notifican con siete días de antelación de la caducidad de la contraseña y se ven forzados a cambiar su contraseña una vez ésta caduca.
QPWDLMTAJC	0 (off)	Limita Digítos Adyacentes en las Contraseñas . 0 (off)- Digitos adyacentes están permitidos en contraseñas 1 (on)- Digitos adyacentes no permitidos en contraseñas
QPWDLMTCHR	#$@	Limita Caracteres Contraseña - Caracteres no válidos en todos los teclados internacionales están restringidos[2]
QPWDLMTREP	2	Limita la repetición en la contraseña - 0-Se permiten caracteres repetidos 1-No se permiten caracteres repetidos 2 No acepta caracteres adyacentes repetidos.
QPWDMAXLEN	10	Máxima Longitud de la Contraseña – Las Contraseñas no pueden ser más largas de ocho (8) lo que significa 10 caracteres de longitud
QPWDMINLEN	6	Mínima Longitud de la Contraseña – Las Contraseñas deben ser de un mínimo de 5 o 6 caracteres de longitud
QPWDPOSDIF	0 (off)	Posición Diferente en la Contraseña – Las contraseñas nuevas pueden tener caracteres en la misma posición que tenían en la contraseña previa.
QPWDRQDDGT	0 (off)	Contraseña requiere dígitos - No se requiren dígitos incluídos en cada contraseña.
QPWDRQDDIF	1	Contraseña Requiere Diferente.- Se requiere que las nuevas contraseñas sean diferentes de las 32 contraseñas anteriores.

[2] Estos caracteres no deberían usarse en los nombres de perfiles de usuario para favorecer el acceso desde cualquier teclado internacional.

Apéndice A: Atributos de Seguridad Global del Sistema-Valores de Sistema

Nombre	Valor Recomendado	Comentarios
QPWDVLDPGM	*NONE	Contraseña de Validación de Programa – No se utiliza contraseña especial de validación de programa además de o en vez de la lógica del estándar OS/400. Si se usa un programa , el programa no debería grabar las contraseñas de usuario (Alta preocupación)

Apéndice B Atributos de Seguridad Global del Sistema –Valores de Red.

Apéndice B Atributos de Seguridad Global del Sistema –Valores de Red.

Tabla 5 Atributos de Red Relativos a Seguridad

Nombre	**Valor Recomendado**	**Comentarios**
JOBACN	**Preferido** *REJECT **Aceptable** *FILE	El atributo de Red JOBACN determina cómo el sistema procesa las peticiones de entrada para ejecutar los trabajos. ***REJECT** La corriente de input se rechaza. Un mensaje que indica que ese input fue rechazado se manda a ambos,al remitente y al destinatario que se intentaba. Si usted no espera recibir peticiones de trabajo remotas en su sistema, configure el atributo de red JOBACN como *REJECT ***FILE** El input se archiva en la cola de ficheros de red para el usuario receptor. Este usuario puede visualizar, cancelar o recibir el input en un fichero de base de datos o someter el trabajo. Se envía al remitente y receptor un mensaje que avisa que el input fue archivado.
PCSACC	**Preferido** *REGFAC	El atributo de Red PCSACC controla si trabajos de PCs pueden acceder a objetos del sistema AS/400 , no si los Pcs pueden usar la emulación de workstation. ***REJECT** El Acceso de los Clientes rechaza cualquier petición de las computadoras para acceder a objetos del AS/400. Se envía un mensaje de error al programa del PC. ***OBJAUT** El Programa de acceso de los clientes en el sistema verifica los permisos normales de los objetos para cualquier objeto solicitado por un programa de PC. ***REGFAC** El sistema usa el registro de sistema para determinar qué programa de salida (si existe alguno) ejecutar. **nombre del programa** El Programa de acceso de los clientes llama a este programa de salida user-written para determinar si las peticiones del PC deben ser permitidas. El programa devuelve un código que indica si la petición seá aceptada o rechazada. Los programas de salida deben ser definidos para permitir la modificación de los ficheros seleccionados para los programas de acceso cliente.

Apéndice B Atributos de Seguridad Global del Sistema –Valores de Red.

Nombre	**Valor Recomendado**	**Comentarios**
DDMACC	nombre del programa	El atributo de Red DDMACC determina como el sistema procesa peticiones desde otros sistemas para acceder a los datos usando la gestión de datos distribuída (DDM) o la función de base de datos relacional distribuída. ***REJECT** El sistema no permite ninguna petición DDM desde sistemas remotos. *REJECT no previene a este sistema de funcionar como sistema de peticiones y enviar peticiones a otrso servidores del sistema. ***OBJAUT** El permiso de los objetos del sistema controla peticiones remotas del sistema. **nombre del programa** Este programa de salida user-written es llamado después que el permiso de objetos normal se ha verficado. El programa de salida es llamado sólo por ficheros DDM , no por funciones de base de datos relacional distribuída. El programa de salida valida las peticiones y envía un código de retorno , garantizando o denegando el acceso solicitado. **El programa de salida para DDMACC puede prevenir comandos remotos desde otros sistemas y usuarios de PC.**

Apéndice C Atributos de Seguridad Global del Sistema – Programas de Salida

Programa 1. Ejemplo Programa de Routing para Batch

```
/*************************************************************/
 /* PURPOSE: ROUTINGPGM - Adopt in batch                      */
 /*    This program can be used as a routing program in batch that   */
 /*    will adopt access so that applications can update production  */
 /*    files.                                                 */
 /*                                                           */
 /*     CRTCLPGM    PGM(ROUTINGxxx  ) USRPRF(*OWNER) LOG(*NO) +      */
 /*                       ALWRTVSRC(*NO)  AUT(*EXCLUDE)       */
 /*     CHGOBJOWN   OBJ(ROUTINGXXX  )  OBJTYPE(*PGM)          */
 /*                       NEWOWN(OWNXXY)                      */
 /*                                                           */
 /*     Grant access to users that will submit jobs to batch  */
 /*     GRTOBJAUT   OBJ(ROUTINGXXX  )  OBJTYPE(*PGM)          */
 /*                       USRPRF(GRPXXY)  AUT(*USE)           */
 /*                                                           */
 /*     The program should adopt a user profile that has the  */
 /*     required authority for access usually SPCAUT(*ALLOBJ) */
 /*                                                           */
 /*  PROGRAMMER                                               */
 /*      Wayne O. Evans         Wayne O. Evans Consulting, Inc */
 /*      Phone (520) 578-7785   Tucson AZ                     */
 /*      Fax   (520) 578-7786   Internet:WOEvans@AOL.com      */
 /*                                                           */
 /*************************************************************/
PGM
             DCL        VAR(&TYPE) TYPE(*CHAR) LEN(1)
             RTVJOBA    TYPE(&TYPE    )
             IF         (&TYPE = '1') RETURN
             CALL QCMD
ENDPGM
```

NOTA: Este programa representa un riesgo potencial para la seguridad si los usuarios están autorizados para llamar a este programa. Para reducir la posibilidad de que este programa sea llamado por usuarios interactivos, el programa se cerrará si no se ejecuta en batch

Apéndice C Atributos de Seguridad Global del Sistema – Programas de Salida

Programa 2. Previene Comandos Remotos y Cargas de Ficheros.

```
/************************************************/
/* Installation instructions                    */
/* 1. Compile program                           */
/*           CRTCLPGM  PGM(LIB/EXIT1)           */
/*                     SRCFILE( ) USRPRF(*OWNER)*/
/* 2. Change owner of the program to user QSECOFR.*/
/*    Adopted authority allows the program sending*/
/*    to the audit journal                      */
/*         CHGOBJOWN OBJ(LIB/EXIT1)             */
/*                   OBJTYPE(*PGM) NEWOWN(QSECOFR)*/
/* 3  Name the exit program in network attributes*/
/*         CHGNETA   DDMACC(LIB/EXIT1)          */
/*                   PCSACC(LIB/EXIT1)          */
/* The audit journal QAUDJRN entries created are:*/
/*   'X1' = Requests that are allowed           */
/*   'X0' = Requests that are rejected          */
/************************************************/
PGM  (&RC  &STRU )
   DCL      &RC    *CHAR   1  /*Return    1=allow    */
                              /*          0=prevent  */
   DCL      &STRU  *CHAR 200  /*Request description  */
   DCL      &USER  *CHAR  10  /*User profile name    */
   DCL      &APP1  *CHAR  10  /*Requested function   */
   DCL      &APP2  *CHAR  10  /*Sub function         */
   DCL      &TYPE  *CHAR   2  /*Journal entry type   */
   MONMSG   CPF0000  EXE(GOTO EXIT) /*If error exit  */
   CHGVAR   &RC    '1'               /*Allow request  */
   CHGVAR   &USER   %SST(&STRU   1 10) /*Get user     */
   CHGVAR   &APP1   %SST(&STRU  11 10) /*Get appl     */
   CHGVAR   &APP2   %SST(&STRU  21 10) /*Get function */
  /*Do not log IBM request to check license  */
  IF (&APP1  =   '*LMSRV')  GOTO EXIT
         /*  Allow all requests for selected users     */
  IF  &USER = 'XXXXXXXXX')  GOTO LOG
        /* Prevent use of remote commands             */
  IF  (&APP1 = '*DDM' *AND &APP2 = 'COMMAND') +
         CHGVAR   &RC '0'   /* Prevent the request    */
  ELSE  /*  Prevent file upload from PC users         */
         /*  File download to PC is not prevented     */
   IF   (&APP1 = '*TFRFCTL' *AND &APP2 = 'REPLACE') +
         CHGVAR   &RC '0'   /* Prevent the request */
        /*  Log request in the audit journal       */
LOG:CHGVAR &TYPE  ( 'X'  *CAT &RC)
```

```
    SNDJRNE  QAUDJRN  TYPE(&TYPE)  &ENTDTA(&STRU)
EXIT:ENDPGM
```

Programa 3. Alternar Programa de Salida para Restringir Transferencia de Ficheros.

```
/*================================================*/
/* Installation instructions:                     */
/* CRTCLPGM  PGM(XXX/EXIT1) SRCFILE(XXX/QCLSRC) +    */
/*           USRPRF(*OWNER)                       */
/* 1. Compile program with adoption owner         */
/* 2. Change owner of the program to user QSECOFR.   */
/*    Adopted authority allows the program sending   */
/*    to the audit journal                        */
/*    CHGOBJOWN  OBJ(XXX/EXIT1A) OBJTYPE(*PGM) +     */
/*               NEWOWN(QSECOFR)                  */
/* 3. Name exit program in registration facility     */
/*    ADDEXITPGM EXITPNT(QIBM_QTF_TRANSFER) +        */
/*             FORMAT(TRAN0100) PGMNBR(1)+          */
/*             PGM(XXX/EXIT1A) +                    */
/* 4. Set registration facility in network attribute */
/*          CHGNETA    PCSACC(*REGFAC)             */
/* The request is recorded in the audit journal      */
/* The audit journal QAUDJRN entries created are:    */
/*   'X1' = requests that are allowed                */
/*   'X0' = requests that are rejected               */
/*================================================*/
PGM        PARM(&RC &STRU)
   DCL  VAR(&RC)    TYPE(*CHAR) LEN(1)
   DCL  VAR(&STRU)  TYPE(*CHAR) LEN(80)
   DCL  VAR(&USER)  TYPE(*CHAR) LEN(10) /* user profile */
   DCL  VAR(&APP1)  TYPE(*CHAR) LEN(10) /* function     */
   DCL  VAR(&APP2)  TYPE(*CHAR) LEN(10) /* sub function */
   DCL  VAR(&TFOBJ) TYPE(*CHAR) LEN(10) /* file  name   */
   DCL  VAR(&TFLIB) TYPE(*CHAR) LEN(10) /* library      */
   DCL  VAR(&TFMBR) TYPE(*CHAR) LEN(10) /* member       */
   DCL  VAR(&TFFMT) TYPE(*CHAR) LEN(10) /* format       */
   DCL  VAR(&TYPE)  TYPE(*CHAR) LEN(2)  /* journal type */
MONMSG     MSGID(CPF0000) EXEC(GOTO CMDLBL(EXIT))
CHGVAR     &RC    VALUE('1') /* set return code to +
              allow request unless rejected by program */
CHGVAR     &USER  VALUE(%SST(&STRU 1 10))  /*user       */
CHGVAR     &APP2  VALUE(%SST(&STRU 21 10)) /*function   */
CHGVAR     &TFOBJ VALUE(%SST(&STRU 31 10)) /*file       */
CHGVAR     &TFLIB VALUE(%SST(&STRU 41 10)) /*library    */
CHGVAR     &TFMBR VALUE(%SST(&STRU 51 10)) /*member     */
CHGVAR     &TFFMT VALUE(%SST(&STRU 61 10)) /*format     */
/*****************************************/
/*  Prevent file upload from PC users      */
/*       except in the UP_LIB library      */
/*****************************************/
IF   (&APP2 *EQ 'REPLACE') *AND +
      (&TFLIB *NE 'UP_LIB    ')  +
         CHGVAR &RC '0') /* prevent the request */
ENDDO
/*****************************************/
/* Log request in the audit journal         */
/*****************************************/
LOG:  CHGVAR     VAR(&TYPE) VALUE('X' *CAT &RC)
  SNDJRNE  JRN(QAUDJRN) TYPE(&TYPE) ENTDTA(&STRU)
```

```
EXIT:ENDPGM
```

Deben ser definidos, un programa de validación de peticiones y un programa de log on en el programa de salida.

- El programa logon debe obligar a cumplir los perfiles de usuario anónimo para la transferencia de ficheros.
- El programa de peticiones debería permitir la descarga de ficheros pero no la carga

Ver la Configuración TCP/IP y la Referencia SC41-5420

Programa 4. FTP Logon

```
/*****************************************************************/
/*   Sample FTP server logon exit program.                       */
/*   Note:  This program is a sample only and has not undergone any */
/*          review or testing.                                   */
/* Additional notes:                                             */
/* 1. When the FTP server logon exit is called, the FTP server job  */
/*    is running under the QTCP user profile.                    */
/* 2. For the ANONYMOUS case, users can add logging capability (for */
/*    example, write the E-mail address entered for the password and*/
/*    the client IP address to a log file).                      */
/* 3. IBM recommends that you create the exit program in a library  */
/*    with *PUBLIC authority of *EXCLUDE,and give the exit program  */
/*    itself a *PUBLIC authority of *EXCLUDE.  The FTP server adopts*/
/*    authority when it is necessary  call the exit program.     */
/*****************************************************************/
TSTLOGCL:PGM  PARM(&APPIDIN &USRIN &USRLENIN &AUTIN &AUTLENIN +
             &IPADDRIN &IPLENIN &RETCDOUT &USRPRFOUT &PASSWDOUT &CURLIBOUT)
/* Declare input parameters */
     DCL       &APPIDIN    *CHAR LEN(4)  /* Application identifier  */
     DCL       &USRIN      *CHAR LEN(999)/* User ID                 */
     DCL       &USRLENIN   *CHAR LEN(4)  /* Length of user ID       */
     DCL       &AUTIN      *CHAR LEN(999)/* Authentication string   */
     DCL       &AUTLENIN   *CHAR LEN(4)  /* Length of auth. string  */
     DCL       &IPADDRIN   *CHAR LEN(15) /* Client IP address       */
     DCL       &IPLENIN    *CHAR LEN(4)  /* IP address length       */
     DCL       &RETCDOUT   *CHAR LEN(4)  /* return code (out)       */
     DCL       &USRPRFOUT  *CHAR LEN(10) /* user profile (out)      */
     DCL       &PASSWDOUT  *CHAR LEN(10) /* password (out)          */
     DCL       &CURLIBOUT  *CHAR LEN(10) /* current library (out)   */
/* Declare local copies of parameters (in format usable by CL) */
          DCL        VAR(&APPID)     TYPE(*DEC)  LEN(1 0)
          DCL        VAR(&USRLEN) TYPE(*DEC) LEN(5 0)
          DCL        VAR(&AUTLEN) TYPE(*DEC) LEN(5 0)
          DCL        VAR(&IPLEN)  TYPE(*DEC) LEN(5 0)
  /* Assign input parameters to local copies */
          CHGVAR     VAR(&APPID)  VALUE(%BINARY(&APPIDIN))
          CHGVAR     VAR(&USRLEN) VALUE(%BINARY(&USRLENIN))
          CHGVAR     VAR(&AUTLEN) VALUE(%BINARY(&AUTLENIN))
          CHGVAR     VAR(&IPLEN)  VALUE(%BINARY(&IPLENIN))
          CHGVAR     VAR(%BINARY(&RETCDOUT)) VALUE(1))
/* Check for ANONYMOUS user. Allow for ANONYMOUS,etc. as  */
/*                           regular user profile. */
          IF         COND(&USRLEN = 9) THEN(DO)
             IF       COND(%SST(&USRIN 1 9) = 'ANONYMOUS') THEN(DO)
/* For anonymous user:force user profile ANONYMOUS               */
/*                    current library to PUBLIC.                 */
```

```
              CHGVAR VAR(%BINARY(&RETCDOUT)) VALUE(6)
              CHGVAR VAR(&USRPRFOUT) VALUE('ANONYMOUS ')
              CHGVAR VAR(&CURLIBOUT) VALUE('PUBLIC    ')
            ENDDO
           ENDDO
/* Any other user: proceed with normal logon processing. */
    END:  ENDPGM
```

Apéndice C Atributos de Seguridad Global del Sistema – Programas de Salida

Programa 5. Programa de Validación de Peticiones para Restringir FTP

Ejemplo de Configuración TCP/IP y Referencia SC41-5420

```
/*****************************************************************/
/*Sample FTP server request validation exit program for anonymous FTP  */
/*Notes:                                                             */
/*1.When the application id is 1 (ftp server) and the operation id is  */
/   0 (session initialization), the job is running under the QTCP      */
/*  User profile when the exit program is called. In all other cases,  */
/*  The job is running under the user's profile.                       */
/*2. Create the exit program in a library with public authority        */
/*  *Exclude.  The exit program itself be given a *EXCLUDE public      */
/*   The FTP server adopts the authority necessary to call the exit    */
/*3. It is possible to use the same exit program for both the ftp      */
/*   Client And server request validation exit points.                 */
/*****************************************************************/
Tstreqcl: pgm  parm(&appidin &opidin &usrprf &ipaddrin +
                    &Iplenin &opinfoin &oplenin &allowop)

/* Declare input parameters */
    DCL  &APPIDIN   *CHAR LEN(4)  /* Application ID              */
    DCL  &OPIDIN    *CHAR LEN(4)  /* Operation ID                */
    DCL  &USRPRF    *CHAR LEN(10) /* User profile                */
    DCL  &IPADDRIN  *CHAR         /* Remote IP address           */
    DCL  &IPLENIN   *CHAR LEN(4)  /* Length of IP address        */
    DCL  &OPLENIN   *CHAR LEN(4)  /* Length of operation-spec info*/
    DCL  &OPINFOIN  *CHAR LEN(9999) /*Operation-specific info     */
    DCL  &ALLOWOP   *CHAR LEN(4)    /* allow (output) */
/* Declare local copies of parameters (in format usable by CL) */
    DCL  &APPID    TYPE(*DEC)  LEN(1 0)
    DCL  &OPID     TYPE(*DEC)  LEN(1 0)
    DCL  &IPLEN    TYPE(*DEC)  LEN(5 0)
    DCL  &IPADDR   *CHAR
    DCL  &OPLEN)   TYPE(*DEC) LEN(5 0)
    DCL  &OPINFO   *CHAR LEN(9999)
    DCL  &PATHNAME *CHAR LEN(9999) /* Uppercase path name        */
  /* Declare values for allow(1) and no allow(0) */
    DCL  &ALLOW    TYPE(*DEC) LEN(1 0) VALUE(1)
    DCL  &NOALLOW  TYPE(*DEC) LEN(1 0) VALUE(0)
  /* Declare request control block for QLGCNVCS (convert case) API*/
  /* convert to uppercase based on job CCSID  */
    DCL  &CASEREQ  *CHAR LEN(22) +
           VALUE(X'00000001000000000000000000000000000000000000')
    DCL   &ERROR *CHAR LEN(4)          VALUE(X'00000000')
/* Assign input parameters to local copies */
   CHGVAR     VAR(&APPID) VALUE(%BINARY(&APPIDIN))
   CHGVAR     VAR(&OPID) VALUE(%BINARY(&OPIDIN))
   CHGVAR     VAR(&IPLEN) VALUE(%BINARY(&IPLENIN))
   CHGVAR     VAR(&IPADDR) VALUE(%SUBSTRING(&IPADDRIN 1 &IPLEN))
   CHGVAR     VAR(&OPLEN) VALUE(%BINARY(&OPLENIN))
/* Handle operation specific information field (which is var Len */
   IF     COND(&OPLEN = 0) THEN(CHGVAR VAR(&OPINFO) VALUE(' '))
   ELSE   CMD(CHGVAR VAR(&OPINFO) VALUE(%SST(&OPINFOIN 1 &OPLEN)))
```

Apéndice C Atributos de Seguridad Global del Sistema – Programas de Salida

```
/* Operation ID 0 (incoming connection): reject if connection is  */
/* through IP accress www.xx.yyy.zzz., accept otherwise.                  */
/* example.) This capability could be used to only allow incoming */
/* connections from an internal network and reject them from the  */   /* "real"
Internet, if the connection to the Internet            */
/* NOTE: For FTP server, operation 0 is ALWAYS under QTCP profile */
   IF         COND(&OPID = 0) THEN(DO)
     IF       COND(&OPINFO = '9.8.7.6') THEN(CHGVAR +
                     VAR(%BINARY(&ALLOWOP)) VALUE(&NOALLOW))
     ELSE     CMD(CHGVAR VAR(%BINARY(&ALLOWOP)) +
                        VALUE(&ALLOW))
     GOTO     CMDLBL(END)
    ENDDO
IF       COND(&USRPRF = 'ANONYMOUS ') THEN(DO)
 /* Do not allow the following operations for ANONYMOUS user:  */
       IF &OPID = 2 | /*Directory/library deletion */ +
                   &OPID = 5 | /* File deletion     */ +
                   &OPID = 7 | /* Receive file      */ +
                   &OPID = 8 | /* Rename file       */ +
                   &OPID = 9   /* Execute cmd       */ +
         THEN(CHGVAR VAR(%BINARY(&ALLOWOP)) VALUE(&NOALLOW))
       ELSE     CMD(DO)
        IF     COND(&OPID = 3 |    /* Change directory       */ +
                 &OPID = 4 |    /* List directory         */ +
                 &OPID = 6 ) DO /* Send file              */
/* Convert path name to uppercase (since names in "root" and */
/*  library file systems are not case sensitive               */
         CALL PGM(QLGCNVCS) PARM(&CASEREQ  &OPINFO +
                                 &PATHNAME &OPLENIN &ERROR)
/* Note: must check for "/public" directory by itself and  */
/*  path names starting  with "/public/".                  */
          IF   COND((%SUBSTRING(&PATHNAME 1 20) *NE +
                '/QSYS.LIB/PUBLIC.LIB') *AND +
                 (&PATHNAME *NE '/PUBLIC') *AND +
                 (%SUBSTRING(&PATHNAME 1 8) *NE '/PUBLIC/')) +
               THEN(CHGVAR VAR(%BINARY(&ALLOWOP)) VALUE(&NOALLOW))
         ELSE CMD(CHGVAR VAR(%BINARY(&ALLOWOP))  VALUE(&ALLOW))
        ENDDO
       ENDDO
    ENDDO
  /* Not ANONYMOUS user:  allow everything  */
    ELSE       CMD(CHGVAR VAR(%BINARY(&ALLOWOP)) VALUE(&ALLOW))
 END:        ENDPGM
```

Apéndice C Atributos de Seguridad Global del Sistema – Programas de Salida

Perfil de Usuario en Programas de Salida

Los programas de Salida están disponibles para operaciones de perfil de usuario.
Crear **Cambiar** **Borrar** **Restaurar**

Los programas de salida pueden llevar a cabo funciones específicas del perfil de usuario como :
Inscribir el perfil de usuario en el directorio del sistema o programa.
Quitar esa alta de un programa para un usuario eliminado.

Programa 6. User Profile Exit Program Shell

```
PGM  (&PARM1)
           DCL  &PARM1      *CHAR   38
           DCL  &EXITNAME   *CHAR   20
           DCL  &FORMAT     *CHAR    8
           DCL  &USRPRF     *CHAR   10
           CHGVAR &EXITNAME %SST(&PARM1  1 20)
           CHGVAR &FORMAT   %SST(&PARM1 21 8 )
           CHGVAR &USRPRF   %SST(&PARM1 29 10)
  CHG:   IF (&FORMAT = CHGP0100 ) DO /*After change */
/*  Add logic here */
           ENDDO
  CRT:   IF (&FORMAT = CRTP0100 ) DO /*After create */
/*  Add enrollment logic here */
           ENDDO
  DLTAFT:IF (&FORMAT = DLTP0100 ) DO /*After delete */
           ENDDO
  DLTBFR:IF (&FORMAT = DLTP0200 ) DO /*Before delete */
/*add application removal logic here  */
           ENDDO
  RST:   IF (&FORMAT = RSTP0100 ) DO /*After restore */
           ENDDO
  ENDPGM
```

Apéndice D: Consideraciones de Seguridad del Acceso ODBC

Las aplicaciones PC tienen la capacidad para leer, modificar e incluso borrar datos de ficheros del AS/400 utilizando ODBC (Open Data Base Connectivity). El diseño habitual de los programas cliente /servidor es el de interactuar con el usuario PC utilizando programas PC. Cuando el programa PC accede a los datos del AS/400, el programa PC utiliza unos interfaces estandarizados (llamadas de programa) para solicitar los datos. Estas peticiones del PC para datos del AS/400 se transforman en peticiones del AS/400 , las cuales se procesan utilizando un trabajo en el AS/400. El perfil de usuario en el trabajo donde las peticiones ODBC se procesan es el perfil de usuario que inicia el router de acceso cliente para el Client Access/400.

La aplicación PC debe tener acceso a ambos, leer y modificar los datos de producción lo que introduce una especial preocupación por la seguridad relativa a cómo se manejan estas peticiones ODBC . Las adopciones de permisos para peticiones ODBC son difíciles y tienen restricciones (ver la alternativa 4 , más adelante). Esta sección describe las diferentes alternativas que permiten el acceso ODBC . Cada una de las sucesivas alternativas es más segura pero requiere más esfuerzo de implementación.

Alternativa 1: Autorizar a los usuarios a los datos.

Implementación: El perfil de usuario que inicia el router Client Access/400 se le da acceso a la actualización de los ficheros de datos de producción. Esto permitirá que cualquier tipo de programa ODBC pueda cambiar los datos.

Si existe la necesidad de auditar los rastros de la información, el AS/400 puede hacer un diario del fichero que está siendo cargado pero esto puede provocar un enorme volume de auditoría si el fichero tiene mucha actividad. Si se requiere auditar a nivel de la aplicación, el programa PC debe utilizar peticiones adicionales ODBC para actualizar los datos de la aplicación auditada.

Consideraciones de Seguridad : Cuando el usuario es autorizado a los datos, el AS/400 no podrá evitar que el usuario utilice otros programas PC (accediendo por fuera del programa) para actualizar los datos de producción.

Autorizar al usuario a los datos puede permitir que el usuario utilice interfaces del AS/400 como query , SQL, y DFU (Data File Utility) para actualizar los datos. Requerir un perfil de usuario distinto para las funciones de acceso cliente que el utilizado para las operaciones interactivas podría eliminar este riesgo. En cualquier caso esto requiere que los usuarios tengan dos perfiles, uno para trabajo interactivo y otro para el trabajo cliente /servidor

El permiso para actualizar los ficheros de datos de producción debería garantizarse sólo para los perfiles de usuario final mejor que para perfiles de grupo. Si el perfil de grupo dispone de acceso ,entonces todos los usuarios del grupo tendrán permitida la actualización a ficheros de producción.

Alternativa 2: Cambiar el Perfil de Usuario en el Programa de Salida.

Implementación: No autorizar al usuario a actualizar los ficheros de datos de producción.Esto elimina el riesgo de , utilizando interfaces AS/400, actualizar los datos de producción y la necesidad de perfiles de usuario separados para acceso Cliente y para interactivo.
Para dar a la aplicación ODBC el acceso que necesita para actualizar los datos de producción, un progarma de salida “canjeará” los perfiles de ususario. Esto es similar a la técnica que se utiliza para la adopción, pero como no permite dicha adopción, el perfil para el trabajo será cambiado.
Consideraciones de Seguridad: El programa de salida no podrá distinguir las peticiones ODBC generadas por la aplicación client aprobada de peticiones similares generadas fuera de la aplicación .Todas las peticiones ODBC (para los perfiles seleccionados) tendrán su perfil *cambiado*.
Las actualizaciones generadas por el trabajo reflejarán la actividad para el perfil de usuario *cambiado* no para el perfil que originó el trabajo.Ambos, el perfil de usuario que inició el trabajo y el perfil de usuario que está ejecutando se grabarán en los registrados de auditoría generados por el sistema.

Alternativa 3: Cambiar el Perfil de Usuario en el Programa de Salida con Autentificación.

Implementación: Esta implementación es una extensión de la alternativa 2. El programa de salida cambiará los perfiles de usuario pero sólo después de que haya habido alguna autentificación. Esta autentificación puede ser en forma de una petición envíada a la base de datos o a la cola de datos que indican que la aplicación está autorizada a realizar actualizaciones de los datos de producción.
Consideraciones de Seguridad: : Esta técnica elimina el riesgo de los interfaces estandarizados del PC, como hojas de cálculo ,tengan permisos para actualizar ficheros de producción.

El método de autentificación tendrá un fuerte código en la aplicación PC y podría ser replicado para ganar acceso por un hacker preparado.En cualquier caso, el riesgo es pequeño.

El cambio de perfiles de usuario tiene las mismas consideraciones de seguridad que las descritas en la opción 2.

Apéndice D: Consideraciones de Seguridad del ODBC

Alternativa 4: Usar procedimientos almacenados.

Implementación: Esta es una forma de adopción de las peticiones ODBC. En vez de permitir peticiones de forma libre , las peticiones pueden ser predefinidas. La petición predefinida se define en un procedimiento almecenado en el AS/400. Los parámetros (teclas de selección) que se pasan al procedimiento llamado se utilizan por la aplicación PC para recuperar o actualizar registros específicos.En vez de generar peticiones ODBC para recuperar y actualizar los datos, la aplicación PC utiliza ODBC para llamar al programa AS/400 que da paso a los datos.

Consideraciones de Seguridad :Esta técnica requiere la creación de procedimientos predefinidos pero resuleve los problemas siguientes :
Los perfiles de usuarios no son cambiados de forma que se simplifica la auditoría de los datos. El usuario que empieza el trabajo se registra en la auditoría como si fueran peticiones interactivas del AS/400 . Si existiesen consideraciones de auditoría , éstas podrían añadirse al programa que implementa el procedimiento predefinido.

Alternativa 5 : Combinación de la opción 3 y 4.

Implementación Esta solución es una modificación que combina los procedimientos almacenados y el cambio de los perfiles de usuario. El esfuerzo de desarrollo (coste) para implementar los procedimientos almacenados para todos los accesos a la base de datos podría reducirse usando el acceso estándar para la mayoría de las peticiones de base de datos. En cualquier caso, un procedimiento almacenado puede utilizarse para autentificar al usuario, en vez de un acceso a la cola de datos, y cambiar el perfil del usuario de forma que peticiones ODBC subsiguientes de la base de datos, se ejecutan con un perfil que está autorizado para modificar los datos de producción.

Consideraciones de Seguridad: Esta técnica requiere la creación de un programa de cambio (SWAP) como el que se muestra en la Figura 6 Program que adopta las autorizaciones *ALLOBJ y *SECADM para cambiar el perfil del usuario . Este programa será llamado por un procedimiento almacenado.El programa de cambio previene un cambio a aquellos perfiles que disponen de accesos poderosos como QSECOFR.

Figura 6 Programa Swap

```
/*****************************************************************/
/*                                                               */
/* Create as user with *ALLOBJ and *SECADM                       */
/*     CRTCLPGM  PGM(lib/SWAP)  USRPRF(*OWNER)  AUT(*EXCLUDE)    */
/*                                                               */
/*                                                               */
/* PURPOSE:   SWAP        --  This program will swap the user    */
/*                            profile of a job but prevents the  */
/*                            swap to a user profile with *ALLOBJ*/
/*                            *SERVICE *SECADM OR *SPLCTL special*/
/*                            authority                          */
/*****************************************************************/
RESETPWD:  PGM (&USERID)
             DCL        &USERID   *CHAR  10
             /*********************************************/
             /* Variables for API to retrieve user profile attributes */
             DCL        &RTNDTA   *CHAR  83
             /*********************************************/
             /*  API work area  USRI0200  data returned     */
             /*********************************************/
             /*        Type       Field                   */
             /*    1   BINARY(4)  Bytes returned          */
             /*    5   BINARY(4)  Bytes available         */
             /*    9   CHAR(10)   User profile name       */
             /*   19   CHAR(10)   User class name         */
             /*   29   CHAR(15)    Special authority      */
             /*   29   CHAR(1 )     ALLOBJ                */
             /*   30   CHAR(1 )     SECADM                */
             /*   31   CHAR(1 )     JOBCTL                */
             /*   32   CHAR(1 )     SPLCTL                */
             /*   33   CHAR(1 )     SAVSYS                */
             /*   34   CHAR(1 )     SERVICE               */
             /*   35   CHAR(1 )     AUDIT                 */
             /*   36   CHAR(1 )     IOSYSCFG              */
             /*   38   CHAR(7 )     future expansion      */
             /*   44   CHAR(10)     Group profile name    */
             /*   54   CHAR(10)     Owner                 */
             /*   64   CHAR(10)     Group authority name  */
             /*   74   CHAR(10)     Limit capabilities    */
             /*********************************************/
             DCL        &OUTVARD  *DEC   (5 0)  VALUE(83)
             DCL        &OUTLEN   *CHAR  4
             DCL        &FMT      *CHAR  8   VALUE(USRI0200)
             DCL        &ERRCDE   *CHAR 80
             DCL        &ERRLEND  *DEC  (5 0)   VALUE(80)
             DCL        &HANDLE   *CHAR  12
```

```
    /*****************************************************/
    /* Retrieve the special authority of the user profile */
    /* Do not allow reset if user has special authority   */
    /*    *ALLOBJ *SECADM *SPLCTL or *SERVICE             */
    /*****************************************************/
    CHGVAR     VAR(%BIN(&OUTLEN)) VALUE(&OUTVARD)
    CHGVAR     VAR(%BIN(&ERRCDE 1 4)) VALUE(&ERRLEND)
    CALL       QSYRUSRI  +
        (&RTNDTA &OUTLEN &FMT &USERID &ERRCDE)
    IF  ( (%SST(&RTNDTA 29 1 )='Y') *OR /*check *ALLOBJ*/ +
          (%SST(&RTNDTA 30 1 )='Y') *OR /*check *SECADM*/ +
          (%SST(&RTNDTA 32 1 )='Y') *OR /*check *SPLCTL*/ +
          (%SST(&RTNDTA 34 1 )='Y')) DO /*check *SERVICE */
        SNDPGMMSG MSGID(CPF9801) MSGTYPE(*ESCAPE) +
         MSGDTA('Swap of this user profile not allowed.')
    ENDDO
/*********************************************************/
/* Swap user profile                                     */
/*********************************************************/
    CALL       QSYGETPH (&USER '*NOPWD' &HANDLE)
    CALL        QWTSETP  ( &HANDLE)
    CALL       QSYRLSPH ( &HANDLE)
ENDPGM
```