IBM

eserver

iSeries

Consejos y herramientas para la seguridad del iSeries

Versión 5

SC10-3122-07

IBM

@server

iSeries

Consejos y herramientas para la seguridad del iSeries

Versión 5

SC10-3122-07

Nota

Antes de utilizar esta información y el producto al que da soporte, asegúrese de leer la información en la sección “Avisos” en la página 177.

Octava edición (Abril 2004)

Esta edición corresponde a la versión 5, release 3, modificación 0 de IBM Operating System/400 (número de producto 5722-SS1) y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones. Esta versión no se ejecuta en todos los modelos de sistema con conjunto reducido de instrucciones (RISC) ni se ejecuta en modelos CISC.

Este manual es la traducción del original en inglés Tips and Tools for Securing your iSeries. Esta edición sustituye a SC10-3122-05 (SC41-5300-06).

Contenido

Figuras

Tablas

Acerca de Consejos y herramientas para la seguridad del iSeries (SC10-3122-07)

El papel que juegan los sistemas informáticos en las empresas está cambiando rápidamente. Los directores de IT, los proveedores de software, los administradores de seguridad y los auditores deben reconsiderar muchos puntos que antes habían dado por supuestos. La seguridad de iSeries se debe incluir en la lista.

Los sistemas proporcionan un gran número de nuevas funciones que son muy distintas de las aplicaciones de contabilidad tradicionales. Los usuarios entran en los sistemas con métodos nuevos: redes LAN, de líneas conmutadas (de marcación), inalámbricas; en resumen, redes de todo tipo. A menudo, los usuarios no ven jamás una pantalla de conexión. Numerosas organizaciones se están convirtiendo en "compañías distribuidas", ya sea con redes propietarias o con Internet.

De pronto parece que los sistemas tienen un conjunto de puertas y ventanas completamente nuevo. Los gestores de sistemas y los administradores de seguridad tienen motivos para estar muy preocupados por la protección de la información en este entorno en cambio constante.

Esta publicación proporciona consejos prácticos para la utilización de las características de seguridad de iSeries y para establecer procedimientos operativos que tengan en cuenta la seguridad. Las recomendaciones de esta publicación son aplicables a una instalación con riesgos y requisitos de seguridad medios. Esta publicación no proporciona una descripción completa de las funciones de seguridad del iSeries disponibles. Si desea consultar las opciones adicionales o necesita una información básica más completa, consulte las publicaciones descritas en Capítulo 17, "Información relacionada", en la página 175.

En esta publicación también se describe cómo configurar y utilizar las herramientas de seguridad que forman parte de OS/400. Capítulo 4, "Configuración del iSeries para utilizar Herramientas de seguridad", en la página 31 y "Mandatos y menús de los mandatos de seguridad" en la página 32 proporcionan información de consulta sobre las herramientas de seguridad. En esta publicación se proporcionan ejemplos de la utilización de dichas herramientas.

A quién está dirigido este manual

El responsable de la seguridad de un sistema es el **responsable de seguridad** o el **administrador de seguridad**. Esta función implica las tareas siguientes:

- Puesta a punto y gestión de los perfiles de usuario
- Definición de valores para todo el sistema que afectan a la seguridad
- Administración de autorización sobre objetos
- Aplicación y supervisión de las estrategias de seguridad

Si es el responsable de la administración de la seguridad de uno o varios sistemas iSeries, esta publicación está dirigida a usted. En las instrucciones de esta publicación se da por supuesto lo siguiente:

- Está familiarizado con los procedimientos de operación básicos de iSeries, como el inicio de sesión y la utilización de mandatos.

- Está familiarizado con los elementos básicos de la seguridad del iSeries: niveles de seguridad, valores del sistema para seguridad, perfiles de usuario y seguridad de objetos.

  Nota: En el Capítulo 1, "Elementos básicos de la seguridad de iSeries", en la página 3 se facilita el resumen de estos elementos. Si estos elementos básicos son nuevos para usted, lea el tema *Seguridad básica y planificación* en el iSeries Information Center. Vea "Requisitos e información relacionada" para obtener más detalles.
- Ha activado la seguridad en el sistema definiendo el valor del sistema de nivel de seguridad (QSECURITY) en 30, como mínimo.

IBM amplía continuamente las funciones de seguridad del iSeries. Para beneficiarse de estas mejoras, es necesario evaluar regularmente el paquete de arreglos acumulativos que esté disponible en cada momento para el release del que disponga. Compruebe si contiene arreglos que conciernan a la seguridad.

Cómo utilizar esta publicación

Si no preparó el sistema para utilizar las herramientas de seguridad o si instaló el Kit de utilidades de seguridad OS/400 de un release anterior, haga lo siguiente:

1. Empiece por el Capítulo 2, "Asistente de seguridad de iSeries y Planificador de seguridad de eServer", en la página 11.En él se describe cómo utilizar estas características para seleccionar las herramientas de seguridad recomendadas y cómo aprender a utilizarlas.
2. Para obtener más información básica sobre la seguridad, puede revisar la información de Consulta de seguridad, que encontrará en línea en iSeries Information Center.

Nota

Esta publicación contiene *muchos* consejos para proteger el iSeries. Es posible que su sistema sólo necesite protección en ciertas áreas. Utilice esta publicación para obtener información sobre los riesgos posibles y sus soluciones. Después centre su atención en las áreas que sean más importantes para su sistema.

Requisitos e información relacionada

Utilice iSeries Information Center como punto de partida para consultar información técnica sobre el iSeries.

Puede acceder al Information Center de dos maneras:

- Desde el siguiente sitio Web:

  `http://www.ibm.com/eserver/iseries/infocenter`
- Desde el CD-ROM *iSeries Information Center*, SK3T-7769-04 (SK3T-4091-04). Este CD-ROM viene con el pedido de hardware de iSeries nuevo o de la actualización de software IBM Operating System/400. También puede pedir el CD-ROM en el IBM Publications Center:

  `http://www.ibm.com/shop/publications/order`

El iSeries Information Center contiene información nueva y actualizada de iSeries, como por ejemplo la instalación de hardware y software, Linux, WebSphere, Java,

alta disponibilidad, base de datos, particiones lógicas, mandatos CL e interfaces de programación de aplicaciones (API) del sistema. Además, ofrece asesores y buscadores para ayudarle a planificar, resolver problemas y configurar el hardware y software de iSeries.

Con cada nuevo pedido de hardware, recibirá *iSeries CD-ROM de instalación y operaciones*, SK3T-4098-02. Este CD-ROM contiene IBM @server IBM e(logo)server iSeries Access para Windows y el asistente EZ-Setup. Familia Access de iSeries ofrece un potente conjunto de posibilidades de cliente y servidor para conectar sistemas PC a servidores iSeries. El asistente EZ-Setup automatiza muchas de las tareas de iSeries.

Cómo enviar sus comentarios

Sus comentarios son importantes para ayudarnos a proporcionar una información precisa y de alta calidad. Si tiene comentarios sobre esta publicación u otra documentación de iSeries, rellene el formulario de comentarios del lector que se encuentra al final de la publicación.

- Si prefiere enviar los comentarios por correo, utilice el formulario de comentarios del lector que lleva impresa la dirección en el reverso. Si envía el formulario de comentarios del lector desde un país que no sea Estados Unidos, puede entregar el formulario a la sucursal local de IBM o al representante de IBM para su envío con franqueo pagado.
- Si prefiere enviar los comentarios por FAX, utilice cualquiera de los números siguientes:
  - Desde Estados Unidos, Canadá y Puerto Rico: 1-800-937-3430
  - Desde otros países: 34 93 321 61 34
- Si prefiere enviar los comentarios por correo electrónico, utilice una de estas direcciones:
  - Comentarios sobre publicaciones:

    RCHCLERK@us.ibm.com
  - Comentarios sobre iSeries Information Center:

    RCHINFOC@us.ibm.com

Asegúrese de incluir lo siguiente:

- El nombre del libro o del tema de iSeries Information Center.
- El número de publicación del libro.
- El número de página o el tema del libro al que hacen referencia sus comentarios.

Parte 1. Seguridad básica de iSeries

Capítulo 1. Elementos básicos de la seguridad de iSeries

Este tema proporciona una breve revisión de los elementos básicos que trabajan conjuntamente para proporcionar seguridad en iSeries. En otras secciones de esta publicación se va más allá de lo básico para proporcionarle consejos para utilizar esos elementos de seguridad de forma que satisfagan las necesidades de su organización.

Niveles de seguridad

Puede elegir la seguridad que desea que tenga el sistema estableciendo el valor del sistema de nivel de seguridad (QSECURITY). El sistema ofrece cinco niveles de seguridad:

Nivel 10:

El sistema no tiene seguridad de ningún tipo. No se precisan contraseñas. Si el perfil de usuario especificado no existe en el sistema cuando se inicia una sesión, el sistema crea uno nuevo.

ATENCIÓN:

A partir de la V4R3 y en futuros releases, no podrá establecer el valor del sistema QSECURITY en 10. Si su sistema tiene actualmente un nivel de seguridad 10, seguirá teniendo el nivel 10 cuando instale la Versión 4 Release 3. Si cambia el nivel de seguridad por otro valor, no podrá regresar al nivel 10. Dado que el nivel 10 no proporciona protección de seguridad, IBM no recomienda el nivel de seguridad 10. **IBM no proporcionará soporte para los problemas que se produzcan con un nivel de seguridad 10, a menos que dicho problema también pueda aparecer con un nivel de seguridad más alto.**

Nivel 20:

El sistema precisa un ID de usuario y una contraseña para el inicio de la sesión. Este nivel también recibe el nombre de **seguridad de inicio de sesión**.Por omisión, todos los usuarios tienen acceso a todos los objetos, ya que poseen la autorización especial *ALLOBJ.

Nivel 30:

El sistema precisa un ID de usuario y una contraseña para el inicio de la sesión. Los usuarios deben tener autorización para la utilización de los objetos, ya que no tienen ninguna autorización por omisión. Esto también se conoce como **seguridad de recursos**.

Nivel 40:

El sistema precisa un ID de usuario y una contraseña para el inicio de la sesión. Además de la seguridad de recursos, el sistema proporciona funciones de **protección de integridad**. Las funciones de protección de la integridad como, por ejemplo, la validación de parámetros para interfaces al sistema operativo, están dirigidas a proteger el sistema y los objetos del mismo contra una mala utilización por parte de los usuarios experimentados. En la mayoría de las instalaciones, el nivel 40 es el nivel

de seguridad recomendable. Cuando reciba un sistema iSeries nuevo con el release V4R5 o uno posterior, el nivel de seguridad estará establecido en 40.

Nivel 50:
El sistema precisa un ID de usuario y una contraseña para el inicio de la sesión. El sistema impone tanto la seguridad por recursos como la protección de integridad del nivel 40,pero añade **protección de integridad mejorada**, como la restricción del manejo de mensajes entre los programas de estado del sistema y los programas de estado de los usuarios. El nivel de seguridad 50 está pensado para los sistemas iSeries con altos requisitos de seguridad.

Nota: El nivel 50 es el nivel necesario para la certificación de C2 (y para la certificación de FIPS-140).

El capítulo 2 de la publicación *iSeries Security Reference* proporciona más información sobre los niveles de seguridad y describe cómo ir de un nivel de seguridad a otro.

Valores globales

Su sistema tiene valores globales que afectan a la manera en que su trabajo entra en el sistema y cómo aparece el sistema ante los demás usuarios del sistema. Estos valores incluyen lo siguiente:

Valores del sistema de seguridad:
Los valores del sistema de seguridad se utilizan para controlar la seguridad en el sistema. Estos valores se dividen en cuatro grupos:
- Valores del sistema de seguridad general
- Otros valores del sistema relacionados con la seguridad
- Valores del sistema que controlan contraseñas
- Valores del sistema que controlan auditorías

Varios temas de esta publicación tratan de las implicaciones de seguridad de ciertos valores del sistema. El capítulo 3 de la publicación *iSeries Security Reference* describe todos los valores del sistema importantes para la seguridad.

Atributos de red:
Los atributos de red controlan el modo en que el sistema participa (o decide no participar) en una red con otros sistemas. Puede obtener más información acerca de los atributos de red leyendo la publicación *Work Management*.

Descripciones de subsistema y otros elementos de gestión de trabajo:
Los elementos de gestión de trabajo determinan la manera en que el trabajo entra en el sistema y el entorno en el que el trabajo se lleva a cabo. Varios temas de esta publicación tratan de las implicaciones de seguridad de ciertos valores de la gestión de trabajo. El manual *Work Management* proporciona información completa.

Configuración de comunicaciones:
La configuración de las comunicaciones también afecta a la manera en que el trabajo entra en el sistema. Varios temas de esta publicación proporcionan sugerencias para proteger el sistema cuando forma parte de una red.

Perfiles de usuario

Cada usuario del sistema **debe** tener un perfil de usuario. Debe crear un perfil de usuario para que un usuario puede iniciar la sesión. Los perfiles de usuario también pueden utilizarse para controlar el acceso a herramientas de servicio tales como DASD y vuelcos del almacenamiento principal. Vea "Gestión de herramientas de servicio" en la página 68 para obtener más información.

El perfil de usuario es una herramienta potente y flexible. Controla las acciones que el usuario puede llevar a cabo y personaliza la manera en que el usuario ve el sistema. La publicación *iSeries Security Reference* describe todos los parámetros del perfil de usuario.

Perfiles de grupo

Un perfil de grupo es un tipo especial de perfil de usuario. Puede utilizarlo para definir la autorización de un grupo de usuarios, en lugar de dar autorización a cada usuario de uno en uno. También puede utilizar un perfil de grupo como patrón al crear perfiles de usuario individuales utilizando la función copiar perfil, o bien, si utiliza iSeries Navigator puede utilizar el menú Políticas de seguridad para editar las autorizaciones de usuario.

El capítulo 5 y el capítulo 7 del manual *iSeries Security Reference* proporcionan información acerca de la planificación y la utilización de perfiles de grupo.

Seguridad por recursos

La seguridad por recursos en el sistema le permite indicar quién puede utilizar los objetos y de qué manera. La posibilidad de acceder a un objeto recibe el nombre de **autorización**. Al establecer la autorización sobre objetos, puede resultar necesario ir con cuidado para otorgar a los usuarios suficiente autorización para realizar su trabajo, pero sin otorgarles autorización para examinar y modificar el sistema. La autorización sobre objetos otorga permisos al usuario para un objeto específico y puede especificar lo que se permite al usuario hacer con el objeto. Un recurso de objeto puede limitarse mediante autorizaciones de usuario específicas detalladas, por ejemplo añadir registro o modificar registros. Pueden utilizarse recursos del sistema para otorgar al usuario acceso subconjuntos de autorizaciones específicas definidas por el sistema: *ALL, *CHANGE, *USE y *EXCLUDE.

Los archivos, programas, bibliotecas y directorios son los objetos del sistema más corrientes que requieren protección de seguridad por recursos, pero puede especificar autorización para cualquier objeto individual del sistema.

En el Capítulo 5, "Protección de la información con la autorización sobre objetos", se trata la importancia de trabajar con la autorización sobre objetos en el sistema. El capítulo 5 del manual *iSeries Security Reference* describe las opciones para la puesta a punto de la seguridad de los recursos.

Acceso limitado a las funciones del programa

La función de acceso limitado a las funciones del programa le permite proporcionar seguridad para el programa cuando no se tiene un objeto iSeries a proteger para el programa. Antes de añadirse el soporte para el acceso limitado a las funciones del programa a la V4R3, podía conseguir el mismo resultado creando una lista de autorizaciones u otro objeto y comparando la autorización con el objeto para controlar el acceso a la función del programa. Ahora puede utilizar el

acceso limitado a las funciones del programa para tener un control más fácil del acceso a una aplicación, a partes de una aplicación o a las funciones de un programa.

Existen dos métodos que puede utilizar para gestionar el acceso de los usuarios a funciones de aplicaciones mediante iSeries Navigator. El primero utiliza el soporte de Administración de las aplicaciones:

1. Pulse con el botón derecho del ratón en el sistema que contenga la función cuyo valor de acceso desee modificar.
2. Seleccione **Administración de aplicaciones**.
3. Si se encuentra en un sistema de administración, seleccione **Valores locales**. De lo contrario, continúe con el paso siguiente.
4. Seleccione una función administrable.
5. Seleccione **Acceso por omisión**, si corresponde. Al realizar esta selección, permite a todos los usuarios acceder a la función por omisión.
6. Seleccione **Acceso a todos los objetos**, si corresponde. Al realizar esta selección, permite a todos los usuarios con privilegio del sistema sobre todos los objetos acceder a esta función.
7. Seleccione **Personalizar**, si corresponde. Utilice los botones **Añadir** y **Eliminar** del diálogo **Personalizar acceso** para añadir o eliminar usuarios o grupos en las listas **Acceso permitido** y **Acceso denegado**.
8. Seleccione **Eliminar personalización**, si corresponde. Al realizar esta selección, suprime el acceso personalizado para la función seleccionada.
9. Pulse en **Aceptar** para cerrar el diálogo **Administración de aplicaciones**.

El segundo método para gestionar el acceso de los usuarios implica el soporte para Usuarios y Grupos de iSeries Navigator:

1. En iSeries Navigator, expanda **Usuarios y grupos**.
2. Seleccione **Todos los usuarios**, **Grupos**, o **Usuarios que no estén en un grupo** para visualizar una lista de usuarios y grupos.
3. Pulse con el botón derecho del ratón en un usuario o en un grupo y seleccione **Propiedades**.
4. Pulse en **Posibilidades**.
5. Pulse en la pestaña **Aplicaciones**.
6. Utilice esta página para cambiar el valor de acceso para un usuario o grupo.
7. Pulse en **Aceptar** dos veces para cerrar el diálogo **Propiedades**.

Vea “Seguridad de iSeries Navigator” en la página 164 para obtener más información sobre los temas de seguridad de iSeries Navigator.

Si se dedica a escribir aplicaciones, puede utilizar las API del acceso limitado a las funciones del programa para efectuar lo siguiente:

- Registrar una función
- Recuperar información acerca de la función
- Definir quién puede utilizar la función y quién no
- Comprobar si al usuario se le permite utilizar la función

Nota: Este soporte **no** sustituye la seguridad por recursos. El acceso limitado a las funciones del programa no evita que un usuario acceda a un recurso (como un archivo o programa) desde otra interfaz.

Para utilizar este soporte dentro de una aplicación, el suministrador de la aplicación deberá registrar las funciones cuando se instale la aplicación. La función registrada se corresponde con un bloque de código dentro de la aplicación, que contiene funciones específicas. Cuando el usuario ejecuta la aplicación, la aplicación llama a la API antes de llamar al bloque de código. La API llama a la API de comprobación de uso para saber si al usuario se le permite utilizar la función. Si se le permite el uso de la función registrada, se ejecuta el bloque de código. Si no se le permite el uso de la función, se niega al usuario la ejecución del bloque de código.

Nota: Las API implican el registro de un ID de función de 30 caracteres en la base de datos de registro (WRKREGINF). Aunque no hay puntos de salida relacionados con los ID de función utilizados por las API de acceso limitado a las funciones, es necesario tener puntos de salida. Para poder registrar algo en el registro, **debe** proporcionar un nombre con formato de punto de salida. Para hacerlo, la API Registrar función crea un nombre ficticio y lo utiliza para todas las funciones que se registren. Dado que se trata de un nombre con formato ficticio, no se llama a ningún programa de punto de salida.

El administrador del sistema especifica quién tiene acceso permitido a una función. El administrador puede utilizar la API para gestionar el acceso a las funciones del programa, o bien utilizar la GUI de la Administración de aplicaciones de iSeries Navigator. La publicación *iSeries Server API Reference* proporciona información sobre el acceso limitado a las API de funciones del programa. Para obtener información adicional sobre el control del acceso a funciones, vea "Seguridad de iSeries Navigator" en la página 164.

Auditorías de seguridad

Los motivos para realizar una auditoría de la seguridad del sistema pueden ser diversos:

- Para evaluar si el plan de seguridad es completo.
- Para asegurarse de que los controles de seguridad planificados están en funcionamiento. Este tipo de auditoría suele realizarla el responsable de seguridad como parte de la administración diaria de la seguridad. También se lleva a cabo, a veces más detalladamente, como parte de una revisión periódica de la seguridad por parte de auditores internos o externos.
- Para asegurarse de que la seguridad del sistema sigue el ritmo de los cambios que se realizan en el entorno del sistema. Estos son algunos ejemplos de los cambios que afectan a la seguridad:
  - Objetos nuevos creados por usuarios del sistema
  - Usuarios nuevos admitidos en el sistema
  - Cambio de la propiedad de objetos (autorización no ajustada)
  - Cambio de responsabilidades (grupo de usuarios modificado)
  - Autorización temporal (no revocada a tiempo)
  - Instalación de nuevos productos
- Para prepararse para un evento futuro como, por ejemplo, instalar una nueva aplicación, ir a un nivel de seguridad superior o configurar una red de comunicaciones.

Las técnicas descritas aquí son apropiadas para todas esas situaciones. Los elementos para los que realice la auditoría y la frecuencia con que lo haga dependerán del tamaño y de las necesidades de seguridad de su organización.

La auditoría de seguridad implica el uso de mandatos en el sistema y el acceso a información de anotaciones y diarios. Puede crear un perfil especial para que lo utilice quien tenga que realizar una auditoría de seguridad de su sistema. El perfil de auditor necesita la autorización especial *AUDIT para modificar las características de auditoría del sistema. Algunas de las tareas de auditoría sugeridas en este capítulo requieren un perfil de usuario con la autorización especial *ALLOBJ y *SECADM. Establezca la contraseña para el perfil de auditor como *NONE al finalizar el periodo de auditoría.

Para obtener más detalles sobre la auditoría de seguridad vea el capítulo 9 de la publicación *Seguridad, Manual de consulta*.

Ejemplo: Informe de atributos de seguridad del sistema

La Figura 1 muestra un ejemplo de la salida del mandato Imprimir atributos de seguridad del sistema (PRTSYSSECA). El informe muestra la configuración de los valores del sistema y los atributos de red relativos a seguridad que se recomiendan para los sistemas con necesidades de seguridad normales. También muestra los valores actuales del sistema.

Nota: La columna *Valor actual* del informe muestra el valor actual del sistema. Compárelo con el valor recomendado para ver dónde puede haber riesgos de seguridad.

```
Atributos de seguridad del sistema

Nombre de valor
del sistema      Valor actual          Valor recomendado
QALWOBJRST       *NONE                 *NONE
QALWUSRDMN       *ALL                  QTEMP
QATNPGM          QEZMAIN   QSYS        *NONE
QAUDENDACN       *NOTIFY               *NOTIFY
QAUDFRCLVL       *SYS                  *SYS
QAUDCTL          *AUDLVL               *AUDLVL   *OBJAUD
QAUDLVL          *SECURITY             *AUTFAIL  *CREATE
                                       *DELETE   *SECURITY
                                       *SAVRST   *NOQTEMP
```

Figura 1. Informe de atributos de seguridad del sistema - Ejemplo (Parte 1 de 4)

```
QAUTOCFG        0                   0
QAUTORMT        1                   0
QAUTOVRT        9999                0
QCMNRCYLMT      0 0                 0 0
QCRTAUT         *CHANGE             Control a nivel de biblioteca.
QCRTOBJAUD      *NONE               Control a nivel de biblioteca.
QDEVRCYACN      *DSCMSG             *DSCMSG
QDSCJOBITV      120                 120
QDSPSGNINF      1                   1
QINACTITV       60                  60
QINACTMSGQ      *ENDJOB             *ENDJOB
QLMTDEVSSN      0                   1
QLMTSECOFR      0                   1
QMAXSGNACN      2                   3
QMAXSIGN        3                   3
```

Figura 1. Informe de atributos de seguridad del sistema - Ejemplo (Parte 2 de 4)

```
QPWDEXPITV      60                  60
QPWDLMTAJC      1                   1
QPWDLMTCHR      *NONE               AEIOU@$#
QPWDLMTREP      1                   2
QPWDLVL         0
QPWDMAXLEN      8                   8
QPWDMINLEN      6                   6
QPWDPOSDIF      1                   1
QPWDRQDDGT      1                   1
QPWDRQDDIF      0                   1
QPWDVLDPGM      *NONE               *NONE
QRETSVRSEC      0                   0
QRMTIPL         0                   0
QRMTSIGN        *FRCSIGNON          *FRCSIGNON
QSECURITY       50                  50
QSHRMEMCTL      1                   0
QSRVDMP         *DMPUSRJOB          *NONE
QUSEADPAUT      *NONE               CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
                                    CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL)
                                    CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)
QVFYOBJRST      1                   3
```

Figura 1. Informe de atributos de seguridad del sistema - Ejemplo (Parte 3 de 4)

```
Atributos de seguridad del sistema

Nombre de
Red             Valor actual        Valor recomendado
DDMACC          *OBJAUT             *REJECT
JOBACN          *FILE               *REJECT
PCSACC          *OBJAUT             *REJECT
```

Figura 1. Informe de atributos de seguridad del sistema - Ejemplo (Parte 4 de 4)

Capítulo 2. Asistente de seguridad de iSeries y Planificador de seguridad de eServer

Las herramientas Asistente de seguridad del servidor iSeries y Planificador de seguridad de eServer pueden ayudarle a decidir los valores de seguridad que debe poner en vigor en el servidor iSeries. Utilizando el Asistente de seguridad del servidor iSeries en iSeries Navigator generará informes que mostrarán las necesidades de seguridad según las respuestas seleccionadas, lo que puede utilizar para configurar la seguridad del sistema.

Utilice el Asistente de seguridad de iSeries o el Planificador de seguridad de eServer como ayuda para planificar e implementar una política de seguridad básica en los servidores iSeries. El objetivo de ambas herramientas es facilitarle la implementación y la gestión de la seguridad en sus sistemas. El asistente, que está disponible como parte de OS/400, le formulará varias preguntas de alto nivel sobre el entorno del servidor y, basándose en sus respuestas, le proporcionará un conjunto de recomendaciones que el asistente puede aplicar al sistema de inmediato.

El Planificador de seguridad de eServer es la versión en línea del Asistente de seguridad. Permite seleccionar opciones basándose en las necesidades de seguridad y genera un informe que sugiere las características necesarias para proteger su sitio.

El Planificador de seguridad de eServer es una versión basada en Web del asistente. Proporciona recomendaciones para implementar la seguridad en el sistema, igual que el asistente. Sin embargo, el asesor no puede aplicar las recomendaciones. En vez de ello, genera una lista de valores de seguridad del sistema y otros atributos que deberá aplicar al sistema, basándose en las respuestas a las preguntas del asesor.

Asistente de seguridad

La decisión sobre qué valores del sistema para la seguridad del iSeries debería utilizar para su empresa puede ser muy compleja. Si no está familiarizado con la implementación de la seguridad en los servidores iSeries, o bien el entorno en el que ejecuta el servidor iSeries ha cambiado recientemente, el Asistente de seguridad puede ayudarle a tomar decisiones.

¿Qué es un asistente?

- Un asistente es una herramienta diseñada para que la utilice un usuario inexperto para instalar o configurar algún elemento en un sistema.
- El asistente solicita información al usuario formulando preguntas. La respuesta a cada pregunta determina qué pregunta se formula a continuación.
- Cuando el asistente ha realizado todas las preguntas, se presenta al usuario un diálogo de finalización. El usuario pulsará entonces el botón **Finalizar** para instalar y configurar el elemento.

Objetivos del Asistente de seguridad

La finalidad del Asistente de seguridad es configurar lo siguiente, basándose en las respuestas de un usuario.

- Valores del sistema y atributos de red relacionados con la seguridad.
- Informes relacionados con la seguridad para la supervisión del sistema
- Generar un Informe de información para el administrador y un Informe de información para el usuario:
  - El Informe de información para el administrador contiene los valores de seguridad recomendados y los procedimientos que deberán seguirse antes de poner en vigor dichas recomendaciones.
  - El Informe de información para el usuario contiene información que puede utilizarse para la política de seguridad de la empresa. Por ejemplo, en este informe se incluyen las normas para componer contraseñas.
- Proporcionar valores recomendados para los diversos elementos del sistema relacionados con la seguridad.

Objetivos del Asistente de seguridad

- Los objetivos del Asistente de seguridad son:
  - Determinar cuáles deben ser los valores de la seguridad del sistema, basándose en las respuestas de los usuarios a las preguntas del asistente y, a continuación, implementar dichos valores cuando sea conveniente.
  - El asistente genera informes de información detallada que incluyen lo siguiente.
    - Informe que explica las recomendaciones del Asistente.
    - Informe que detalla los procedimientos que deberán seguirse antes de la implementación.
    - Informe que lista información importante que debe distribuirse a los usuarios del sistema.
- Estos elementos ponen en vigor en el sistema la política de seguridad básica.
- El asistente recomienda informes de diario de auditoría que deberá planificar para que se ejecuten periódicamente. Una vez planificados, estos informes ayudan a lo siguiente:
  - Asegurar que se siguen las políticas de seguridad.
  - Asegurar que las políticas de seguridad sólo se modifican con su aprobación.
  - Planificar informes para supervisar los eventos del sistema relacionados con la seguridad.
- El asistente le permite guardar las recomendaciones o aplicarlas todas o parte de ellas al sistema.

Nota: El Asistente de seguridad puede utilizarse más de una vez en el mismo sistema para permitir a los usuarios que tengan una instalación más antigua revisar su seguridad actual. El Asistente de seguridad puede utilizarse en los sistemas de la V3R7 (cuando apareció iSeries Navigator) y posteriores.

Para poder utilizar iSeries Navigator, debe tener instalado IBM iSeries Access para Windows en el PC Windows 95/NT y tener una conexión con el servidor iSeries desde dicho PC. El usuario del Asistente debe estar conectado a un servidor iSeries. El usuario debe tener un ID de usuario que tenga las autorizaciones especiales *ALLOBJ, *SECADM, *AUDIT y *IOSYSCFG. Para obtener ayuda sobre la conexión del PC Windows 95/NT al sistema iSeries, consulte el tema IBM iSeries Access para Windows en Information Center (vea “Requisitos e información relacionada” en la página xii para conocer más detalles).

Para acceder al Asistente de seguridad, haga lo siguiente:

1. En iSeries Navigator, expanda el servidor.
2. Pulse con el botón derecho del ratón en **Seguridad** y seleccione **Configurar**.

- Cuando un usuario inicia la opción **Seguridad** de iSeries Navigator, se envía una petición al servidor iSeries para comprobar la autorización especial del usuario.
- Si el usuario no tuviera todas las autorizaciones especiales necesarias (*ALLOBJ, *AUDIT, *IOSYSCFG, *SECADM), no podrá ver la opción **Configurar** y no podrá acceder al Asistente de seguridad.

3. Suponiendo que el usuario tenga la autorización necesaria:
   - Se recuperan las respuestas anteriores del asistente.
   - Se recuperan los valores de seguridad actuales.

El Asistente de seguridad le presentará una de tres pantallas de bienvenida. La pantalla que vea dependerá de cuál de estas condiciones se cumpla:

- No se ha ejecutado nunca el asistente para el servidor iSeries destino.
- El asistente se ha ejecutado antes y los cambios en la seguridad se han diferido.
- El asistente se ha ejecutado antes y los cambios en la seguridad entraron en vigor.

Si no está utilizando iSeries Navigator, igualmente puede obtener ayuda para planificar las necesidades de seguridad. El Planificador de seguridad de eServer es una versión en línea del Asistente de seguridad, con una diferencia. El asesor no configurará el sistema automáticamente. Sin embargo, generará un informe sobre las opciones de seguridad recomendadas basándose en sus respuestas. Para acceder al Planificador de seguridad de eServer, vaya al eServer Information Center:

`http://publib.boulder.ibm.com/eserver/`

Planificador de seguridad de eServer

El Planificador de seguridad de eServer es una versión en línea del Asistente de seguridad. Formula las mismas preguntas que el Asistente de seguridad y, según sus respuestas, genera las mismas recomendaciones. Las diferencias principales entre ambas herramientas son:

- El Planificador de seguridad de eServer **no** hace lo siguiente—
  - Generar informes.
  - Comparar los valores actuales con los valores recomendados.
  - Establecer cualquier valor del sistema automáticamente.
- No puede aplicar las recomendaciones desde el Planificador de seguridad de eServer.

El Planificador de seguridad de eServer genera un programa CL que puede cortar y pegar, o editar para su propio uso, con el fin de automatizar la configuración de la seguridad. También puede enlazar directamente con la documentación del servidor iSeries desde el Planificador de seguridad de eServer. Esta documentación proporciona información acerca del valor del sistema o informe que le ayudará a determinar si dicho valor es el apropiado para su entorno.

Para acceder al Planificador de seguridad de eServer, apunte el navegador Internet al siguiente URL:

`http://publib.boulder.ibm.com/eserver/`

Capítulo 3. Control del inicio de sesión interactivo

Cuando se plantee restringir la entrada al sistema, comience con lo más obvio: la pantalla Inicio de sesión. A continuación se enumeran las opciones que puede utilizar para dificultar a extraños la posible conexión a su sistema utilizando la pantalla Inicio de sesión.

Definir normas para contraseñas

Para proteger la conexión al sistema, haga lo siguiente:
- Adopte una política que establezca que las contraseñas no deben ser obvias y que no se deben compartir.
- Establezca valores del sistema para facilitar su aplicación. En la Tabla 1 se muestran los valores del sistema recomendados.

La combinación de valores en la Tabla 1 es muy restrictiva y está pensada para reducir de forma significativa la posibilidad de que haya contraseñas fácilmente deducibles. Sin embargo, los usuarios pueden encontrar difícil y frustrante el seleccionar una contraseña que cumpla estas restricciones.

Considere la posibilidad de proporcionar a los usuarios lo siguiente:
1. Una lista de los criterios para las contraseñas.
2. Ejemplos de contraseñas válidas y no válidas.
3. Sugerencias para escoger una contraseña adecuada.

Ejecute el mandato Configurar seguridad del sistema (CFGSYSSEC) para fijar estos valores. Utilice el mandato Imprimir atributos de seguridad del sistema (PRTSYSSECA) para imprimir la definición actual de estos valores del sistema.

El capítulo 3 de la publicación *iSeries Security Reference*. El apartado "Valores establecidos por el mandato Configurar seguridad del sistema" en la página 42 proporciona más información sobre el mandato CFGSYSSEC.

Tabla 1. Valores del sistema para las contraseñas

Nombre del valor del sistema	Descripción	Valor recomendado
QPWDEXPITV	Frecuencia con la que los usuarios del sistema deben cambiar las contraseñas. Puede especificar un valor distinto para cada usuario en el perfil de usuario.	60 (días)
QPWDLMTAJC	Indica si el sistema impedirá que haya caracteres adyacentes iguales.	1 (sí)
QPWDLMTCHR	Caracteres que no pueden utilizarse en las contraseñas. [2]	AEIOU#$@
QPWDLMTREP	Indica si el sistema impedirá que aparezca el mismo carácter más de una vez en la contraseña.	2 (no se permiten de forma consecutiva)
QPWDLVL	Indica si las contraseñas de perfil de usuario están limitadas a 10 caracteres o a un máximo de 128.	0[3]
QPWDMAXLEN	Número máximo de caracteres de una contraseña.	8
QPWDMINLEN	El número mínimo de caracteres de que debe constar una contraseña.	6
QPWDPOSDIF	Indica si todos los caracteres de una contraseña deben ser distintos del carácter que ocupaba la misma posición en la contraseña anterior.	1 (sí)

Tabla 1. Valores del sistema para las contraseñas (continuación)

Nombre del valor del sistema	Descripción	Valor recomendado
QPWDRQDDGT	Indica si la contraseña debe tener un carácter numérico como mínimo.	1 (sí)
QPWDRQDDIF	Tiempo que debe esperar un usuario para poder volver a utilizar la misma contraseña.[2]	5 o menos (intervalos de caducidad)[1]
QPWDVLDPGM	Indica a qué programa de salida se llama para validar una contraseña recién asignada.	*NONE

Notas:

1. El valor del sistema QPWDEXPITV especifica la frecuencia con la que debe cambiarse la contraseña (por ejemplo, cada 60 días). Recibe el nombre de **intervalo de caducidad**. El valor del sistema QPWDRQDDIF especifica los intervalos de caducidad que deben pasar para que se pueda volver a utilizar la contraseña. En el Capítulo 3 de la publicación *iSeries Security Reference* se proporciona más información acerca del funcionamiento conjunto de estos valores del sistema.
2. QPWDLMTCHR no se impone en los niveles de contraseña 2 ó 3. Vea "Niveles de contraseña" para conocer más detalles.
3. Consulte "Planificación de cambios de nivel de contraseña" en la página 17 para determinar el nivel de contraseña adecuado a sus necesidades.

Niveles de contraseña

A partir de la V5R1 del sistema operativo, el valor del sistema QPWDLVL ofrece una mayor seguridad en las contraseñas. En los releases anteriores, los usuarios estaban limitados a contraseñas de un máximo de 10 caracteres y con un rango de caracteres limitado. Ahora los usuarios pueden seleccionar una contraseña (o frase de paso) con un máximo de 128 caracteres, dependiendo del nivel de contraseña en el que esté establecido el sistema. Los niveles de contraseña son:

- **Nivel 0:** Los sistemas se envían con este nivel. En el nivel 0, las contraseñas no tienen más de 10 caracteres de longitud y contienen solamente los caracteres A-Z, 0–9, #, @, $, y _ . Las contraseñas del nivel 0 son menos seguras que las de los niveles de contraseña superiores.
- **Nivel 1:** Las mismas normas que en el nivel de contraseña 0, pero no se guardan las contraseñas para el Soporte de iSeries para Windows Network Neighborhood (a partir de ahora conocido como iSeries NetServer).
- **Nivel 2:** Las contraseñas están protegidas en este nivel. Este nivel puede utilizarse para pruebas. Las contraseñas se salvan para un usuario en el nivel 0 ó 1 si son de 10 caracteres o menos y utilizan el juego de caracteres para contraseñas de nivel 0 ó 1. Las contraseñas (o frases de paso) de este nivel tienen las siguientes características:
  - un máximo de 128 caracteres de longitud.
  - se componen de cualquier carácter disponible en el teclado.
  - no pueden constar completamente de blancos; los blancos se eliminan del final de la contraseña.
  - son sensibles a mayúsculas y minúsculas.
- **Nivel 3:** Las contraseñas de este nivel son las más seguras y utilizan los algoritmos de cifrado más avanzados disponibles. Las contraseñas de este nivel tienen las mismas características que en el nivel 2. Las contraseñas para iSeries NetServer no se guardan en este nivel.

Solamente debe utilizar los niveles de contraseña 2 y 3 si todos los sistemas de su red cumplen estos criterios:

- El sistema operativo es de la V5R1 o posterior
- El nivel de contraseña está establecido en 2 ó 3

De forma similar, todos los usuarios deben conectarse utilizando el mismo nivel de contraseña. Los niveles de contraseña son globales; los usuarios no pueden elegir el nivel en el que les gustaría proteger su contraseña.

Planificación de cambios de nivel de contraseña

El cambio de niveles de contraseña debe planificarse cuidadosamente. Es posible que las operaciones que se efectúen con otros sistemas fallen o que los usuarios no puedan iniciar la sesión en el sistema si no ha planificado el cambio de nivel de contraseña correctamente. Antes de modificar el valor del sistema QPWDLVL, asegúrese de que ha salvado los datos de seguridad utilizando el mandato SAVSECDTA o SAVSYS. Si tiene una copia de seguridad actualizada, podrá restablecer las contraseñas para todos los perfiles de usuario si resulta necesario volver a un nivel de contraseña inferior.

Los productos que utilice en el sistema y en los clientes con los que el sistema intercambie información podrían tener problemas cuando el valor del sistema de nivel de contraseña (QPWDLVL) esté establecido en 2 ó 3. Cualquier producto o cliente que envíe contraseñas al sistema en formato cifrado, en lugar de en el texto claro que un usuario entra en una pantalla de inicio de sesión, deberá actualizarse para trabajar con las nuevas normas de cifrado de contraseñas para QPWDLVL 2 ó 3. El envío de contraseñas cifradas se denomina **sustitución de contraseña**.

La sustitución de contraseña se utiliza para evitar que se capture una contraseña durante la transmisión por una red. No se aceptarán las sustituciones de contraseñas generadas por clientes antiguos que no soporten el nuevo algoritmo para QPWDLVL 2 ó 3, incluso si los caracteres específicos tecleados son correctos. Esto también es aplicable al acceso de cualquier iSeries a otro iSeries igual que utilice los valores cifrados para realizar autenticación de un sistema a otro.

El problema se agrava por el hecho de que algunos de los productos afectados (por ejemplo Java Toolbox) se proporcionan como middleware. Un producto de terceros que incorpore una versión anterior de uno de estos productos no funcionará correctamente hasta que se reconstruya utilizando una versión actualizada del middleware.

Dado este y otros ejemplos prácticos, es fácil ver por qué es necesaria una planificación minuciosa antes de modificar el valor del sistema QPWDLVL.

Consideraciones para cambiar QPWDLVL de 0 a 1

El nivel de contraseña 1 permite a un sistema, que no tiene necesidad de comunicarse con el producto Windows 95/98/ME AS/400 Client Support para Windows Network Neighborhood (iSeries NetServer), hacer que se eliminen las contraseñas de iSeries NetServer del sistema. Eliminar las contraseñas cifradas innecesarias del sistema aumenta la seguridad global del sistema.

En QPWDLVL 1, todos los mecanismos actuales de contraseña y autenticación de contraseña anteriores a la V5R1 seguirán funcionando. Hay pocas probabilidades de interrupciones, excepto en las funciones y servicios que requieran contraseñas de iSeries NetServer.

Consideraciones para cambiar QPWDLVL de 0 ó 1 a 2

El nivel de contraseña 2 introduce el uso de contraseñas sensibles a mayúsculas y minúsculas de hasta 128 caracteres (también denominadas frases de paso) y proporciona la capacidad máxima de volver a QPWDLVL 0 ó 1.

Independientemente del nivel de contraseña del sistema, las contraseñas del nivel 2 y 3 se crean siempre que se modifica una contraseña o un usuario inicia la sesión en el sistema. La creación de una contraseña de nivel 2 y 3 mientras el sistema aún sigue en el nivel de contraseña 0 ó 1 ayuda a prepararse para el cambio al nivel de contraseña 2 ó 3.

Antes de cambiar QPWDLVL a 2, deberá utilizar los mandatos DSPAUTUSR o PRTUSRPRF TYPE(*PWDINFO) para localizar todos los perfiles de usuario que no tengan una contraseña utilizable en el nivel de contraseña 2. Dependiendo de los perfiles localizados por estos mandatos, puede interesarle utilizar uno de los siguientes mecanismos para hacer que se añada una contraseña de nivel de contraseña 2 y 3 a los perfiles.

- Cambiar la contraseña para el perfil de usuario utilizando el mandato CL CHGUSRPRF o CHGPWD o la API QSYCHGPW. Esto provocará que el sistema cambie la contraseña utilizable en los niveles de contraseña 0 y 1; el sistema también creará dos contraseñas equivalentes sensibles a mayúsculas y minúsculas que son utilizables en los niveles de contraseña 2 y 3. Se crea además una versión en mayúsculas y otra en minúsculas de la contraseña para su uso en el nivel de contraseña 2 ó 3.

  Por ejemplo, cambiar la contraseña a C4D2RB4Y da como resultado que el sistema genere las contraseñas C4D2RB4Y y c4d2rb4y del nivel de contraseña 2.
- Iniciar la sesión en el sistema mediante un mecanismo que presente la contraseña en texto claro (no se utiliza la sustitución de contraseña). Si la contraseña es válida y el perfil de usuario no tiene una contraseña utilizable en los niveles de contraseña 2 y 3, el sistema crea dos contraseñas equivalentes sensibles a mayúsculas y minúsculas utilizables en los niveles de contraseña 2 y 3. Se crea además una versión en mayúsculas y otra en minúsculas de la contraseña para su uso en el nivel de contraseña 2 ó 3.

La ausencia de una contraseña utilizable en el nivel de contraseña 2 ó 3 puede ser un problema cuando el perfil de usuario tampoco tenga una contraseña utilizable en los niveles de contraseña 0 y 1, o cuando el usuario intente iniciar la sesión a través de un producto que utilice sustitución de contraseña. En estos casos, el usuario no podrá iniciar la sesión cuando se cambie el nivel de contraseña a 2.

Si un perfil de usuario no tiene una contraseña utilizable en los niveles de contraseña 2 y 3, pero tiene una contraseña utilizable en los niveles de contraseña 0 y 1 y el usuario inicia la sesión a través de un producto que envíe contraseñas de texto claro, el sistema validará el usuario ante la contraseña del nivel de contraseña 0 y creará dos contraseñas del nivel de contraseña 2 (tal como se describe más arriba) para el perfil de usuario. Los siguientes inicios de sesión se validarán ante las contraseñas del nivel de contraseña 2.

Cualquier cliente/servicio que utilice sustitución de contraseña no funcionará correctamente en QPWDLVL 2 si no se ha actualizado el cliente/servicio para que utilice el nuevo esquema de sustitución de contraseña. El administrador deberá comprobar si es necesario un cliente/servicio que no se haya actualizado al nuevo esquema de sustitución de contraseña.

Los clientes/servicios que utilizan la sustitución de contraseña incluyen:

- TELNET
- iSeries Access
- iSeries Host Servers
- QFileSrv.400
- Soporte de impresión de iSeries NetServer
- DDM
- DRDA
- SNA LU6.2

Es altamente recomendable salvar los datos de seguridad antes de cambiar a QPWDLVL 2. Ello puede ayudar a que el retorno a QPWDLVL 0 ó 1 sea más fácil, si fuera necesario.

Se recomienda también que no se cambien los demás valores del sistema para contraseñas, QPWDMINLEN y QPWDMAXLEN, hasta que se hayan realizado pruebas en QPWDLVL 2. Esto facilitará el retorno a QPWDLVL 1 ó 0, si es necesario. No obstante, el valor del sistema QPWDVLDPGM debe especificar *REGFAC o *NONE para que el sistema pueda permitir que se cambie QPWDLVL a 2. Por consiguiente, si utiliza un programa de validación de contraseñas, puede interesarle escribir uno nuevo que pueda registrarse para el punto de salida QIBM_QSY_VLD_PASSWRD utilizando el mandato ADDEXITPGM.

Las contraseñas de iSeries NetServer siguen estando soportadas en QPWDLVL 2, por lo que cualquier función/servicio que requiera una contraseña de iSeries NetServer deberá seguir funcionando correctamente.

Una vez el administrador se sienta cómodo ejecutando el sistema en QPWDLVL 2, puede empezar a cambiar los valores del sistema de las contraseñas para la explotación de contraseñas más largas. No obstante, el administrador debe tener en cuenta que las contraseñas más largas pueden provocar estos efectos:

- Si se especifican contraseñas de más de 10 caracteres, se borrará la contraseña del nivel de contraseña 0 y 1. Este perfil de usuario no podrá iniciar la sesión si se devuelve el sistema al nivel de contraseña 0 ó 1.
- Si las contraseñas contienen caracteres especiales o no siguen las normas de composición para nombres de objeto simples (excluida la sensibilidad a mayúsculas y minúsculas), se borrará la contraseña del nivel de contraseña 0 y 1.
- Si se especifican contraseñas de más de 14 caracteres, se borrará la contraseña de iSeries NetServer del perfil de usuario.
- Los valores del sistema para contraseñas solamente son aplicables al nuevo valor de nivel de contraseña 2 y no a los valores de contraseña de los niveles de contraseña 0 y 1 generados por el sistema o de iSeries NetServer (si se han generado).

Consideraciones para cambiar QPWDLVL de 2 a 3

Tras ejecutar el sistema en QPWDLVL 2 durante algún tiempo, el administrador puede considerar el ir a QPWDLVL 3 para maximizar la protección de seguridad por contraseñas.

En QPWDLVL 3 se borran todas las contraseñas deiSeries NetServer por lo que un sistema no debería pasar a QPWDLVL 3 hasta que no haya necesidad de utilizar contraseñas de iSeries NetServer.

En QPWDLVL 3 se borran todas las contraseñas de los niveles de contraseña 0 y 1. El administrador puede utilizar los mandatos DSPAUTUSR o PRTUSRPRF para localizar los perfiles de usuario que no tengan asociados contraseñas del nivel de contraseñas 2 ó 3.

Cambio a un nivel de contraseña inferior

Aunque es posible volver a un valor de QPWDLVL inferior, no puede esperarse que resulte una operación sin problemas. La idea general es que se trata de un proceso en una dirección solamente, de los valores de QPWDLVL inferiores a los valores de QPWDLVL superiores. No obstante, pueden darse casos en los que deba reinstaurarse un valor de QPWDLVL inferior.

Las secciones siguientes tratan las tareas necesarias para volver a un nivel de contraseña inferior.

Consideraciones para cambiar de QPWDLVL 3 a 2: Este cambio es relativamente fácil. Una vez QPWDLVL esté establecido en 2, el administrador debe determinar si algún perfil de usuario debe contener contraseñas de iSeries NetServer o contraseñas del nivel de contraseña 0 ó 1 y, si hay alguno, cambiar la contraseña del perfil de usuario a un valor permitido.

Adicionalmente, puede ser necesario volver a cambiar los valores del sistema para contraseñas a valores compatibles con contraseñas de iSeries NetServer y de nivel de contraseña 0 ó 1, si son necesarias dichas contraseñas.

Consideraciones para cambiar de QPWDLVL 3 a 1 ó 0: Debido a las altas probabilidades de provocar problemas en el sistema (por ejemplo, que nadie pueda iniciar la sesión al haberse borrado todas las contraseñas de los niveles de contraseña 0 y 1), este cambio no está soportado directamente. Para cambiar de QPWDLVL 3 a QPWDLVL 1 ó 0, el sistema debe pasar primero por el cambio intermedio a QPWDLVL 2.

Consideraciones para cambiar de QPWDLVL 2 a 1: Antes de cambiar QPWDLVL a 1, el administrador deberá utilizar los mandatos DSPAUTUSR o PRTUSRPRF TYPE(*PWDINFO) para localizar los perfiles de usuario que no tengan una contraseña del nivel de contraseña 0 ó 1. Si el perfil de usuario va a necesitar una contraseña una vez de haya cambiado el QPWDLVL, el administrador deberá asegurarse de que se crea una contraseña del nivel de contraseña 0 y 1 para el perfil, utilizando uno de los siguientes mecanismos:

- Cambiar la contraseña para el perfil de usuario utilizando el mandato CL CHGUSRPRF o CHGPWD o la API QSYCHGPW. Esto provocará que el sistema cambie la contraseña utilizable en los niveles de contraseña 2 y 3; el sistema también creará una contraseña equivalente en mayúsculas que sea utilizable en los niveles de contraseña 0 y 1. El sistema sólo será capaz de crear la contraseña de los niveles de contraseña 0 y 1 si se cumplen las siguientes condiciones:
  - La contraseña tiene 10 caracteres o menos de longitud.
  - La contraseña puede convertirse a los caracteres EBCDIC en mayúsculas A-Z, 0-9, @, #, $ y subrayado.
  - La contraseña no empieza por un carácter numérico o subrayado.

  Por ejemplo, cambiar la contraseña a un valor de DíaLluvia daría como resultado que el sistema generase una contraseña de los niveles de contraseña 0 y 1 de DIALLUVIA. Pero cambiar el valor de contraseña a Días de Lluvia de

Abril provocaría que el sistema borrase la contraseña de los niveles de contraseña 0 y 1 (debido a que la contraseña es demasiado larga y contiene espacios en blanco).

No se genera ningún mensaje ni indicación si no ha podido crearse la contraseña del nivel de contraseña 0 ó 1.

- Iniciar la sesión en el sistema mediante un mecanismo que presente la contraseña en texto claro (no se utiliza la sustitución de contraseña). Si la contraseña es válida y perfil de usuario no tiene una contraseña utilizable en los niveles de contraseña 0 y 1, el sistema crea una contraseña equivalente en mayúsculas que sea utilizable en los niveles de contraseña 0 y 1. El sistema sólo será capaz de crear la contraseña de los niveles de contraseña 0 y 1 si se cumplen las condiciones listadas más arriba.

El administrador podrá entonces cambiar QPWDLVL a 1. Se borrarán todas las contraseñas de iSeries NetServer cuando entre en vigor el cambio a QPWDLVL 1 (la siguiente IPL).

Consideraciones para cambiar de QPWDLVL 2 a 0: Las consideraciones son las mismas que para cambiar de QPWDLVL 2 a 1, excepto que se conservan todas las contraseñas de iSeries NetServer cuando el cambio entra en vigor.

Consideraciones para cambiar de QPWDLVL 1 a 0: Tras cambiar QPWDLVL a 0, el administrador deberá utilizar los mandatos DSPAUTUSR o PRTUSRPRF para localizar los perfiles de usuario que no tengan una contraseña de iSeries NetServer. Si el perfil de usuario requiere una contraseña de iSeries NetServer, ésta puede crearse modificando la contraseña del usuario o iniciando la sesión mediante un mecanismo que presente la contraseña en texto claro.

El administrador podrá entonces cambiar QPWDLVL a 0.

Cambio de contraseñas conocidas

Efectúe lo siguiente para impedir el acceso fácil al servidor iSeries con contraseñas que pueden seguir existiendo en el sistema.

__ Paso 1. Asegúrese de que ningún perfil de usuario tiene la contraseña por omisión (que coincide con el nombre del perfil de usuario). Puede utilizar el mandato Analizar contraseñas por omisión (ANZDFTPWD). (Vea el apartado “Evitar contraseñas por omisión” en la página 27.)

__ Paso 2. Intente iniciar la sesión en el sistema con las combinaciones de perfiles de usuario y contraseñas enumeradas en la Tabla 2 en la página 22. Estas contraseñas están publicadas y son la primera elección de cualquiera que intente entrar en su sistema sin permiso. Si puede iniciar la sesión, utilice el mandato Cambiar perfil de usuario (CHGUSRPRF) para cambiar la contraseña por el valor recomendado.

__ Paso 3. Arranque las Herramientas de Servicio Dedicado (DST) e intente iniciar la sesión con las contraseñas mostradas en Tabla 2 en la página 22. Consulte iSeries Information Center—>Seguridad—>Herramientas de servicio. Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

__ Paso 4. Si puede iniciar la sesión en DST con alguna de estas contraseñas, deberá cambiar las contraseñas. iSeries Information Center—>Seguridad—>Herramientas de servicio, proporcionan instrucciones detalladas sobre cómo cambiar los ID de usuario y las

contraseñas de las herramientas de servicio. Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

__ Paso 5. Finalmente, asegúrese de que no puede iniciarse la sesión pulsando la tecla Intro en la pantalla Inicio de sesión sin entrar un ID de usuario y una contraseña. Pruebe en varias pantallas. Si puede iniciar la sesión sin entrar información alguna en la pantalla Inicio de sesión, efectúe una de estas acciones:

- Cambie el valor de seguridad por 40 ó 50 (valor del sistema QSECURITY).

  Nota: Las aplicaciones se pueden ejecutar de modo diferente al aumentar el nivel de seguridad a 40 ó 50.

- Cambie todas las entradas de estación de trabajo para subsistemas interactivos de modo que señalen a las descripciones de trabajos en las que se especifica USER(*RQD).

Tabla 2. Contraseñas para perfiles suministrados por IBM

ID de usuario	Contraseña	Valor recomendado
QSECOFR	QSECOFR[1]	Valor no deducible, conocido únicamente por el administrador de seguridad. **Anote la contraseña elegida y guárdela en un lugar seguro.**
QSYSOPR	QSYSOPR	*NONE[2]
QPGMR	QPGMR	*NONE[2]
QUSER	QUSER	*NONE[2, 3]
QSRV	QSRV	*NONE[2]
QSRVBAS	QSRVBAS	*NONE[2]

Notas:

1. El sistema se envía con el valor *Establecer contraseña como caducada* para QSECOFR establecido como *YES. La primera vez que se inicia la sesión en un sistema nuevo, debe cambiar la contraseña de QSECOFR.
2. El sistema necesita estos perfiles de usuario para las funciones del sistema, pero no debe permitir que los usuarios inicien la sesión con estos perfiles. Para sistemas nuevos instalados con la V3R1 o un release posterior, esta contraseña se envía como *NONE.

   Cuando se ejecuta el mandato CFGSYSSEC, el sistema establece estas contraseñas como *NONE.
3. Para ejecutar iSeries Access para Windows utilizando TCP/IP, debe habilitarse el perfil de usuario QUSER.

Tabla 3. Contraseñas para herramientas de servicio dedicado

Nivel de DST	ID de usuario[1]	Contraseña	Valor recomendado
Funciones básicas	11111111	11111111	Un valor no deducible, conocido únicamente por el administrador de seguridad.[2]
Todas las funciones	22222222	22222222[3]	Un valor no deducible, conocido únicamente por el administrador de seguridad.[2]
Funciones de seguridad	QSECOFR	QSECOFR[3]	Un valor no deducible, conocido únicamente por el administrador de seguridad.[2]

Tabla 3. Contraseñas para herramientas de servicio dedicado (continuación)

Nivel de DST	ID de usuario[1]	Contraseña	Valor recomendado
Posibilidad de servicio	QSRV	QSRV[3]	Un valor no deducible, conocido únicamente por el administrador de seguridad.[2]

Notas:

1. Solamente se requiere un ID de usuario para los releases PowerPC AS (RISC) del sistema operativo.
2. Si el representante de servicio de hardware necesita conectarse con esta contraseña e ID de usuario, cambie la contraseña para un nuevo valor una vez que el servicio técnico de hardware haya terminado.
3. El perfil de usuario de las herramientas de servicio caducará en cuanto se haya utilizado por primera vez.

Nota: Las contraseñas DST sólo pueden modificarse mediante un dispositivo autenticado. Esto también se cumple para todas las contraseñas y los ID de usuario correspondientes que sean idénticos. Para obtener más información sobre los dispositivos autenticados, consulte la información de configuración de la Consola de operaciones en iSeries Information Center.

Establecimiento de valores de inicio de sesión

En la Tabla 4 se muestran diversos valores que se pueden definir para que a una persona no autorizada le resulte más difícil la conexión al sistema. Si ejecuta el mandato CFGSYSSEC, estos valores del sistema tomarán los valores recomendados. Puede leer más acerca de estos valores del sistema en el Capítulo 3 de la publicación *iSeries Security Reference*.

Tabla 4. Valores del sistema de inicio de sesión

Nombre del valor del sistema	Descripción	Valor recomendado
QAUTOCFG	Indica si el sistema configura automáticamente nuevos dispositivos.	0 (No)
QAUTOVRT	Número de descripciones de dispositivos virtuales que el sistema creará automáticamente si no hay ningún dispositivo disponible para su utilización	0
QDEVRCYACN	Qué hace el sistema cuando se vuelve a conectar un dispositivo después de un error.[1]	*DSCMSG
QDSCJOBITV	Cuánto tiempo espera el sistema antes de finalizar un trabajo desconectado.	120
QDSPSGNINF	Indica si el sistema visualizará información acerca de la actividad de inicio de sesión previa cuando un usuario se conecta.	1 (Sí)
QINACTITV	Cuánto tiempo espera el sistema antes de realizar alguna acción cuando un trabajo interactivo está inactivo.	60
QINACTMSGQ	Qué acción lleva a cabo el sistema cuando se alcanza el período de tiempo de QINACTITV.	*ENDJOB
QLMTDEVSSN	Indica si el sistema impedirá a los usuarios iniciar una sesión en más de una estación de trabajo simultáneamente.	1 (Sí)

Tabla 4. Valores del sistema de inicio de sesión (continuación)

Nombre del valor del sistema	Descripción	Valor recomendado
QLMTSECOFR	Indica si los usuarios que disponen de la autorización especial *ALLOBJ o *SERVICE pueden iniciar la sesión solamente en estaciones de trabajo determinadas.	1 (Sí)[2]
QMAXSIGN	Número máximo de intentos consecutivos de inicio de sesión incorrectos (el perfil de usuario o la contraseña son incorrectos).	3
QMAXSGNACN	Acción que el sistema lleva a cabo cuando se alcanza el límite de QMAXSIGN.	3 (Inhabilitar el perfil de usuario y el dispositivo)

Notas:

1. El sistema puede desconectar y volver a conectar sesiones TELNET cuando se ha asignado explícitamente la descripción de dispositivo para la sesión.
2. Si establece este valor del sistema en 1 (Sí), será necesario otorgar autorización sobre los dispositivos explícitamente a los usuarios que disponen de las autorizaciones especiales *ALLOBJ o *SERVICE. El modo más sencillo de hacerlo es proporcionar al perfil de usuario QSECOFR la autorización *CHANGE sobre dispositivos determinados.

Cambio de mensajes de error de inicio de sesión

A los piratas informáticos les resulta muy útil saber si van por buen camino cuando tratan de entrar en un sistema sin permiso. Cuando en la pantalla Inicio de sesión se visualiza un mensaje de error que dice `Contraseña incorrecta`, el pirata informático sabe que el ID de usuario sí es correcto. Puede intentar despistarle utilizando el mandato Cambiar descripción de mensaje (CHGMSGD) para modificar el texto de dos mensajes de error de inicio de sesión. La Tabla 5 contiene el texto que se recomienda utilizar.

Tabla 5. Mensajes de error de inicio de sesión

ID de mensaje	Texto enviado	Texto recomendado
CPF1107	CPF1107 – Contraseña incorrecta para perfil de usuario.	La información de inicio de sesión no es correcta. **Nota:** No incluya el ID de mensaje en el texto.
CPF1120	CPF1120 – El usuario `XXXXX` no existe.	La información de inicio de sesión no es correcta. **Nota:** No incluya el ID de mensaje en el texto.

Planificación de la disponibilidad de perfiles de usuario

Es posible que desee que algunos perfiles de usuario estén disponibles solamente a determinadas horas del día o en ciertos días de la semana. Por ejemplo, si tiene un perfil configurado para un supervisor de seguridad, puede habilitarlo solamente durante las horas de trabajo previstas del supervisor. También puede inhabilitar perfiles de usuario con autorización especial *ALLOBJ (incluido el perfil de usuario QSECOFR) durante el horario no de oficina.

Puede utilizar el mandato Cambiar entrada de planificación de activación (CHGACTSCDE) para establecer que los perfiles de usuarios se puedan habilitar e

inhabilitar automáticamente. Para cada perfil de usuario que desee planificar, debe crear una entrada que defina la planificación del perfil de usuario.

Por ejemplo, si desea que el perfil QSECOFR esté disponible únicamente entre las 7 de la mañana y las 10 de la noche, escribirá lo siguiente en la pantalla CHGACTSCDE:

```
         Cambiar entrada de planificación de activación (CHGACTSCDE)

 Teclee elecciones, pulse Intro.

Perfil de usuario  . . . . . > QSECOFR       Nombre
Hora habilitación  . . . . . > '7:00'        Hora, *NONE
Hora inhabilitación  . . . . > '22:00'       Hora, *NONE
Días . . . . . > *MON          *ALL, *MON, *TUE, *WED...
                               > *TUE
                               > *WED
                               > *THU
             + para más valores > *FRI
```

Figura 2. Pantalla de planificación de activación de perfil–Ejemplo

De hecho, quizá desee disponer del perfil QSECOFR sólo para un número limitado de horas cada día. Puede utilizar otro perfil de usuario con la clase *SECOFR para realizar la mayoría de las funciones. De este modo, evitará arriesgar un perfil de usuario conocido ante los piratas informáticos.

Puede utilizar periódicamente el mandato Visualizar entradas de diario de auditoría (DSPAUDJRNE) para imprimir las entradas CP (Cambiar perfil) de diario de auditoría. Utilice estas entradas para verificar que el sistema habilita e inhabilita los perfiles de usuario según la planificación efectuada.

Otro método para asegurarse de que los perfiles de usuario se inhabilitan de acuerdo con lo planificado es la utilización del mandato Imprimir perfil de usuario (PRTUSRPRF). Cuando se especifica *PWDINFO para el tipo de informe, el informe incluye el estado de cada perfil de usuario seleccionado. Si, por ejemplo, inhabilita regularmente todos los perfiles de usuario que tienen la autorización especial *ALLOBJ, puede planificar el mandato siguiente para que se ejecute inmediatamente después de la inhabilitación de los perfiles:

```
PRTUSRPRF TYPE(*PWDINFO) SELECT(*SPCAUT) SPCAUT(*ALLOBJ)
```

Eliminación de perfiles de usuario inactivos

El sistema debe contener solamente los perfiles de usuario que sean necesarios. Si ya no necesita un perfil de usuario porque el usuario ya no trabaja en su organización o porque ocupa otro cargo en la misma, elimine el perfil de usuario. Si alguien está ausente de la organización durante un amplio período de tiempo, inhabilite (desactive) el perfil de usuario correspondiente. Los perfiles de usuario innecesarios pueden constituir un modo de entrar en el sistema sin autorización para ello.

Inhabilitación automática de perfiles de usuario

Puede utilizar el mandato Analizar actividad de perfil (ANZPRFACT) para inhabilitar regularmente los perfiles de usuario que han estado inactivos durante un número determinado de días. Cuando se utiliza el mandato ANZPRFACT, se

especifica el número de días de inactividad que buscará el sistema. El sistema consulta la fecha del último uso, la fecha de restauración y la fecha de creación del perfil de usuario.

Una vez haya especificado un valor para el mandato ANZPRFACT, el sistema planificará un trabajo para que se ejecute semanalmente a la 1 del mediodía (empezando el día después de que se especificara un valor por primera vez). El trabajo examina todos los perfiles e inhabilita los perfiles inactivos. No es preciso que utilice de nuevo el mandato ANZPRFACT, a menos que desee cambiar el número de días de inactividad.

Puede utilizar el mandato Cambiar lista de perfiles activos (CHGACTPRFL) para hacer que algunos perfiles estén exceptuados del proceso de ANZPRFACT. El mandato CHGACTPRFL crea una lista de perfiles de usuario que el mandato ANZPRFACT no inhabilitará, independientemente del tiempo que hayan estado inactivos.

Cuando el sistema ejecuta el mandato ANZPRFACT graba una entrada CP en el diario de auditoría para cada perfil de usuario que se inhabilita. Puede utilizar el mandato DSPAUDJRNE para listar los perfiles de usuario que se acaban de inhabilitar.

Nota: El sistema solamente graba entradas de auditoría si en el valor QAUDCTL se especifica *AUDLVL y en el valor del sistema QAUDLVL se especifica *SECURITY.

Otro método para asegurarse de que los perfiles de usuario se inhabilitan de acuerdo con lo planificado es la utilización del mandato Imprimir perfil de usuario (PRTUSRPRF). Cuando se especifica *PWDINFO para el tipo de informe, se incluye en éste el estado de todos los perfiles de usuario seleccionados.

Eliminación automática de perfiles de usuario

Puede utilizar el mandato Cambiar entrada de planificación de caducidad (CHGEXPSCDE) para gestionar la eliminación o la inhabilitación de perfiles de usuario. Si sabe que un usuario estará ausente durante un amplio período de tiempo, puede planificar la eliminación o la inhabilitación del perfil de usuario correspondiente.

La primera vez que se utiliza el mandato CHGEXPSCDE, se crea una entrada de planificación de trabajo que se ejecuta cada día un minuto después de la medianoche. El trabajo consulta el archivo QASECEXP para determinar si se ha planificado la eliminación de perfiles de usuario ese día.

Con el mandato CHGEXPSCDE, puede inhabilitar o suprimir un perfil de usuario. Si opta por suprimirlo, debe indicar qué acciones llevará a cabo el sistema con los objetos propiedad del usuario. Antes de planificar la supresión de un perfil de usuario, es necesario investigar los objetos que son propiedad de ese usuario. Por ejemplo, si el usuario es propietario de programas que adoptan autorización, ¿desea que estos programas adopten la autorización del nuevo propietario? ¿O el nuevo propietario tiene más autorización de la necesaria (por ejemplo, autorización especial)? Quizá necesite crear un nuevo perfil de usuario con autorizaciones especiales para poseer programas para los que se necesita autorización.

También es necesario averiguar si se producirán problemas en las aplicaciones al suprimir ese perfil de usuario. Por ejemplo, ¿en alguna de las descripciones de trabajo se especifica ese perfil de usuario como usuario por omisión?

Puede utilizar el mandato Visualizar planificación de caducidad (DSPEXPSCD) para visualizar la lista de perfiles que se han planificado para su inhabilitación o eliminación.

Puede utilizar el mandato Visualizar usuarios autorizados (DSPAUTUSR) para obtener una lista de todos los perfiles de usuario del sistema. Utilice el mandato Suprimir perfil de usuario (DLTUSRPRF) para suprimir los perfiles antiguos.

Nota de seguridad:: Los perfiles de usuario se inhabilitan estableciendo su estado como *DISABLED. Cuando se inhabilita un perfil, deja de estar disponible para su uso interactivo. No puede iniciar la sesión ni cambiar un trabajo utilizando un perfil de usuario inhabilitado. Los trabajos de proceso por lotes sí se pueden ejecutar bajo un perfil de usuario que esté inhabilitado.

Evitar contraseñas por omisión

Cuando se crea un nuevo perfil de usuario, se toma como contraseña por omisión el mismo nombre del perfil. Ello proporciona una oportunidad de entrar en el sistema sin permiso, si el intruso conoce su método de asignación de nombres de perfil y sabe que se unirá un nuevo miembro a su organización.

Cuando cree perfiles de usuario nuevos, considere la posibilidad de asignarles contraseñas exclusivas y no deducibles en lugar de utilizar la contraseña por omisión. Informe al nuevo usuario de cuál es su contraseña de forma confidencial; por ejemplo, en una carta de bienvenida al sistema en la que se indica cuáles son sus métodos de seguridad. Haga que el usuario cambie la contraseña la primera vez que inicie la sesión estableciendo el perfil de usuario con el valor PWDEXP(*YES).

Puede utilizar el mandato Analizar contraseñas por omisión (ANZDFTPWD) para comprobar si en el sistema hay perfiles de usuario con contraseñas por omisión. Cuando imprima el informe, tendrá la opción de especificar que el sistema debe emprender alguna acción (como la inhabilitación del perfil de usuario) si la contraseña coincide con el nombre del perfil de usuario. El mandato ANZDFTPWD imprime una lista de los perfiles que encontró y las acciones que llevó a cabo.

Nota: Las contraseñas se almacenan en el sistema en un formato cifrado irreversible. No se pueden descifrar. El sistema cifra la contraseña especificada y la compara con la contraseña almacenada, tal como comprobaría una contraseña cuando iniciara la sesión en el sistema. Si está realizando una auditoría de las anomalías de autorización (*AUTFAIL), el sistema grabará una entrada de diario de auditoría PW para cada perfil de usuario que *no* tenga una contraseña por omisión (para los sistemas con V4R1 o releases anteriores). A partir de la V4R2, el sistema no graba entradas de diario de auditoría PW cuando se ejecuta el mandato ANZDFTPWD.

Supervisión de la actividad de inicio de sesión y de contraseña

Si le preocupan los intentos de entrar en el sistema sin autorización, puede utilizar el mandato PRTUSRPRF para supervisar la actividad de inicio de sesión y de contraseña.

A continuación se enumeran varias sugerencias para utilizar este informe:

- Determine si el intervalo de caducidad de la contraseña para algunos perfiles de usuario es superior al valor del sistema y si ello está justificado. Por ejemplo, en el informe, USERY tiene un intervalo de caducidad de contraseña de 120 días.
- Ejecute este informe regularmente para supervisar los intentos de inicio de sesión no satisfactorios. Aquellas personas que intenten entrar sin permiso en su sistema pueden darse cuenta de que el sistema lleva a cabo alguna acción tras un cierto número de intentos no satisfactorios. Cada noche, el intruso potencial podría intentar el inicio de sesión menos veces de las especificadas en el valor QMAXSIGN para evitar que se descubra su intención. Sin embargo, si ejecuta este informe cada mañana y observa que determinados perfiles suelen tener intentos de inicio de sesión no satisfactorios, puede empezar a pensar que pueden surgir problemas.
- Identifique los perfiles de usuario que no se han utilizado o cuyas contraseñas no se han cambiado durante mucho tiempo.

Almacenamiento de información de contraseñas

Para dar soporte a algunos requisitos de comunicaciones y funciones de red, los servidores iSeries proporcionan un método seguro para almacenar las contraseñas que se pueden descifrar. El sistema utiliza estas contraseñas, por ejemplo, para establecer una conexión SLIP con otro sistema. (En el apartado “Seguridad y sesiones de marcación de salida” en la página 137 se describe esta utilización de las contraseñas almacenadas.)

Los servidores iSeries almacenan estas contraseñas especiales en un área segura que no es accesible a las interfaces ni a los programas de usuario. Solamente las funciones del sistema con autorización explícita pueden establecer y recuperar estas contraseñas.

Por ejemplo, cuando se utiliza una contraseña almacenada para las conexiones SLIP de marcación, la contraseña se establece con el mandato del sistema que crea el perfil de configuración (WRKTCPPTP). Es preciso tener *IOSYSCFG para utilizar este mandato. Un script de conexión codificado de forma especial recupera la contraseña y la descifra durante el procedimiento de marcación. La contraseña descifrada no es visible para el usuario ni en ninguna anotación de trabajo.

Como administrador de seguridad, debe decidir si permitirá que en el sistema se almacenen las contraseñas que se puedan descifrar. Para especificarlo, utilice el valor del sistema Retener datos de seguridad del servidor (QRETSVRSEC). El valor por omisión es 0 (No). Por lo tanto, el sistema no almacenará contraseñas que pueden descifrarse si no establece explícitamente este valor del sistema.

Si tiene requisitos de comunicaciones o de redes para las contraseñas almacenadas, debe definir los métodos adecuados y comprender los métodos y las prácticas de las organizaciones con las que se comunica. Por ejemplo, cuando se utiliza SLIP para comunicarse con otro servidor iSeries, en ambos sistemas debe tenerse en cuenta la preparación de perfiles de usuario especiales para establecer las sesiones.

Dichos perfiles deben tener autorización limitada sobre el sistema. De este modo se limita el efecto sobre el sistema si una contraseña almacenada está comprometida en un sistema asociado.

Capítulo 4. Configuración del iSeries para utilizar Herramientas de seguridad

Este apartado describe cómo realizar la puesta a punto del sistema para utilizar las herramientas de seguridad que forman parte de OS/400. Cuando instala el OS/400, las herramientas de seguridad están listas para ser utilizadas. Los temas que siguen proporcionan sugerencias para los procedimientos operativos con las herramientas de seguridad.

Operación de Herramientas de seguridad con seguridad

Cuando se instala OS/400, los objetos asociados con las herramientas de seguridad están protegidos. Para trabajar con las herramientas de seguridad de una forma correcta, evite hacer cambios de autorización a los objetos de herramientas de seguridad.

A continuación se indican los requisitos y valores de seguridad para los objetos de herramientas de seguridad:

- Los programas y mandatos de las herramientas de seguridad están en la biblioteca del producto QSYS. Los mandatos y los programas se entregan con la autorización de uso público de *EXCLUDE. Muchos de los mandatos de las herramientas de seguridad crean archivos en la biblioteca QUSRSYS. Cuando el sistema crea estos archivos, la autorización de uso público para los archivos es *EXCLUDE.

  Los archivos que contienen información para producir informes cambiados tienen nombres que empiezan por QSEC. Los archivos que contienen información para gestionar perfiles de usuario tienen nombres que empiezan por QASEC. Estos archivos contienen información confidencial acerca del sistema. Por tanto, no debe cambiar la autorización de uso público sobre los archivos.
- Las herramientas de seguridad utilizan la puesta a punto normal del sistema para dirigir la salida impresa. Estos informes contienen información confidencial acerca del sistema. Para dirigir la salida a una cola de salida protegida, haga los cambios oportunos en el perfil de usuario o descripción de trabajo para los usuarios que ejecutarán las herramientas de seguridad.
- Debido a sus funciones de seguridad y a que tienen acceso a muchos objetos del sistema, los mandatos de las herramientas de seguridad requieren autorización especial *ALLOBJ. Algunos de los mandatos también requieren autorización especial *SECADM, *AUDIT o *IOSYSCFG. Para asegurarse de que los mandatos se ejecutan satisfactoriamente, debe iniciar la sesión como responsable de seguridad cuando utilice las herramientas de seguridad. Por tanto, no es necesario que otorgue autorización privada a ningún mandato de las herramientas de seguridad.

Evitar conflictos de archivos

Muchos de los mandatos de informe de las herramientas de seguridad crean un archivo de base de datos que se puede utilizar para imprimir una versión modificada del informe. El apartado “Mandatos y menús de los mandatos de seguridad” en la página 32 le indica el nombre de archivo para cada mandato.Sólo puede ejecutar un mandato a la vez desde un trabajo. Actualmente la mayoría de

los mandatos tienen métodos para hacer que esto se cumpla. Si ejecuta un mandato cuando otro trabajo aún no ha terminado de ejecutarlo, recibirá un mensaje de error.

Muchos trabajos de impresión son trabajos de larga ejecución. Hay que tener cuidado para evitar conflictos de archivo cuando los informes se someten a procesos por lotes o cuando se añaden al planificador de trabajos. Por ejemplo, es posible que desee imprimir dos versiones del informe PRTUSRPRF con diferentes criterios de selección. Si está sometiendo informes a proceso por lotes, debe utilizar una cola de trabajos que no ejecute más de un trabajo al mismo tiempo, para asegurarse de que los trabajos de informes se ejecutan secuencialmente.

Si está utilizando un planificador de trabajos, debe planificar los dos trabajos con suficiente separación para que la primera versión finalice antes de que se inicie el segundo trabajo.

Salvar Herramientas de seguridad

Los programas de las herramientas de seguridad se guardan siempre que se ejecute el mandato Salvar sistema (SAVSYS) o una opción del menú Salvar que ejecuta el mandato SAVSYS.

Los archivos de las herramientas de seguridad están en la biblioteca QUSRSYS. Esta biblioteca se debe salvar como parte de los procedimientos operativos que se realizan habitualmente. La biblioteca QUSRSYS contiene datos para muchos programas bajo licencia del sistema. Consulte el Information Center para obtener más información sobre qué mandatos y opciones salvan la biblioteca QUSRSYS.

Mandatos y menús de los mandatos de seguridad

Este apartado describe los mandatos y los menús para las herramientas de seguridad. A lo largo de esta publicación encontrará ejemplos sobre el modo de utilizar los mandatos.

Existen dos menús disponibles para las herramientas de seguridad:

- El menú SECTOOLS (Herramientas de seguridad) para ejecutar mandatos de forma interactiva.
- El menú SECBATCH (Someter o planificar informes de seguridad para procesar por lotes) para ejecutar los mandatos del informe por lotes. El menú SECBATCH está dividido en dos partes. La primera parte del menú utiliza el mandato Someter trabajo (SBMJOB) para someter informes para el proceso por lotes inmediato.

  La segunda parte del menú utiliza el mandato Añadir entrada de planificación de trabajos (ADDJOBSCDE). Se utiliza para planificar los informes de seguridad para ejecutarlos regularmente a la hora y el día especificados.

Opciones del menú Herramientas de seguridad

La Tabla 6 en la página 33 describe las opciones de menú y los mandatos asociados:

Tabla 6. Mandatos de herramientas para perfiles de usuario

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
1	ANZDFTPWD	Utilice el mandato Analizar contraseñas por omisión para informar y emprender una acción en los perfiles de usuario que tienen una contraseña que es igual que el nombre de perfil de usuario.	QASECPWD[2]
2	DSPACTPRFL	Utilice el mandato Visualizar lista de perfiles activos para visualizar o imprimir la lista de perfiles de usuario que están exentos del proceso de ANZPRFACT.	QASECIDL[2]
3	CHGACTPRFL	Utilice el mandato Cambiar lista de perfiles activos para añadir y eliminar perfiles de usuario de la lista de exenciones para el mandato ANZPRFACT. Un perfil de usuario que se encuentra en la lista de perfiles activos está permanentemente activo (hasta que se elimine el perfil de la lista). El mandato ANZPRFACT no inhabilita un perfil que se encuentre en la lista de perfiles activos, por mucho tiempo que el perfil haya permanecido inactivo.	QASECIDL[2]
4	ANZPRFACT	Utilice el mandato Analizar actividad de perfil para inhabilitar los perfiles de usuario que no se han utilizado durante un número especificado de días. Después de utilizar el mandato ANZPRFACT para especificar el número de días, el sistema ejecuta el trabajo ANZPRFACT por la noche. Puede utilizar el mandato CHGACTPRFL para impedir que los perfiles de usuario se inhabiliten.	QASECIDL[2]
5	DSPACTSCD	Utilice el mandato Visualizar planificación de activación de perfil para visualizar o imprimir información sobre la planificación para habilitar e inhabilitar los perfiles de usuario específicos. La planificación se crea con el mandato CHGACTSCDE.	QASECACT[2]
6	CHGACTSCDE	Utilice el mandato Cambiar entrada de planificación de activación para que un perfil de usuario esté disponible para iniciar la sesión solamente en determinados momentos del día o de la semana. Para cada perfil de usuario que se planifica, el sistema crea entradas de planificación de trabajos para las horas de habilitación e inhabilitación.	QASECACT[2]
7	DSPEXPSCD	Utilice el mandato Visualizar planificación de caducidad para visualizar o imprimir la lista de los perfiles de usuario que se han planificado para la inhabilitación o eliminación del sistema en el futuro. El mandato CHGEXPSCDE se utiliza para preparar la caducidad de los perfiles de usuario.	QASECEXP[2]

Tabla 6. Mandatos de herramientas para perfiles de usuario (continuación)

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
8	CHGEXPSCDE	Utilice el mandato Cambiar entrada de planificación de caducidad para planificar la eliminación de un perfil de usuario. Puede eliminarlo temporalmente (inhabilitándolo) o puede suprimirlo del sistema. Este mandato utiliza una entrada de planificación de trabajos que se ejecuta cada día a las 00:01 (1 minuto después de la medianoche). El trabajo examina el archivo QASECEXP para determinar si algún perfil de usuario se ha establecido para que caduque ese día. Utilice el mandato DSPEXPSCD para visualizar los perfiles de usuario cuya caducidad se ha planificado.	QASECEXP[2]
9	PRTPRFINT	Utilice el mandato Imprimir información interna de perfil para imprimir un informe que contiene información sobre el número de entradas contenidas en un perfil de usuario. El número de entradas determina el tamaño del perfil de usuario.	

Notas:

1. Las opciones pertenecen al menú SECTOOLS.
2. Este archivo está en la biblioteca QUSRSYS.

Puede avanzar páginas en el menú para ver las opciones adicionales. La Tabla 7 en la página 35 describe las opciones de menú y los mandatos asociados para las auditorías de seguridad:

Tabla 7. Mandatos de herramientas para la auditoría de seguridad

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
10	CHGSECAUD	Utilice el mandato Cambiar auditoría de seguridad para poner a punto la auditoría de seguridad y cambiar los valores del sistema que la controlan. Cuando se ejecuta el mandato CHGSECAUD, el sistema crea el diario de auditoría de seguridad (QAUDJRN), en caso de que no exista. El mandato CHGSECAUD proporciona opciones que simplifican la definición del valor del sistema QAUDLVL (nivel de auditoría). Puede especificar *ALL para activar todos los posibles valores del nivel de auditoría. También puede especificar *DFTSET para activar los valores utilizados más comúnmente (*AUTFAIL, *CREATE, *DELETE, *SECURITY y *SAVRST). **Nota:** Si utiliza las herramientas de seguridad para poner a punto la auditoría, asegúrese de planificar la gestión de los receptores de diario de auditoría. De lo contrario podrá encontrarse rápidamente con problemas relativos a la utilización del disco.	
11	DSPSECAUD	Utilice el mandato Visualizar auditoría de seguridad para visualizar información sobre el diario de auditoría de seguridad y los valores del sistema que controlan la auditoría de seguridad.	

Notas:

1. Las opciones pertenecen al menú SECTOOLS.

Utilización del menú Proceso por lotes de la seguridad

A continuación, le presentamos la primera parte del menú SECBATCH:

```
SECBATCH  Someter o planificar informes seguridad para procesar por lotes
                                                                Sistema:
Seleccione una de las siguientes opciones:

  Someter informes para procesar por lotes
    1. Adopción de objetos
    2. Entradas de diario de auditoría
    3. Autorizaciones de la lista de autorizaciones
    4. Autorización de mandato
    5. Autorización de uso privado sobre mandato
    6. Seguridad de comunicaciones
    7. Autorización sobre directorio
    8. Autorización de uso privado sobre directorio
    9. Autorización sobre documento
   10. Autorización de uso privado sobre documento
   11. Autorización sobre archivo
   12. Autorización de uso privado sobre archivo
   13. Autorización sobre carpeta
```

Cuando se selecciona una opción de este menú, aparece una pantalla Someter trabajo (SBMJOB). Si desea modificar las opciones por omisión del mandato, puede pulsar F4 (Solicitud) en la línea *Mandato a ejecutar*.

Para ver Someter informes a proceso por lotes, avance página en el menú SECBATCH. Utilizando las opciones de esta parte del menú, puede por ejemplo, preparar el sistema para que ejecute con regularidad las versiones modificadas de los informes. Puede avanzar páginas para ver más opciones de menú. Cuando se selecciona una opción de esta parte del menú, se visualiza la pantalla Añadir entrada de planificación de trabajos (ADDJOBSCDE).

Puede situar el cursor en la línea *Mandato a ejecutar* y pulsar F4 (Solicitud) para elegir diferentes valores para el informe. Debe asignar un nombre de trabajo que tenga sentido para poder reconocer la entrada cuando se visualizan entradas de planificación de trabajos.

Opciones del menú Proceso por lotes de la seguridad

La Tabla 8 describe las opciones de menú y los mandatos asociados para los informes de seguridad.

Cuando ejecuta los informes de seguridad, el sistema sólo imprime información que se ajusta a los criterios de selección que ha especificado y a los criterios de selección de la herramienta. Por ejemplo, las descripciones de trabajo que especifican un nombre de perfil de usuario son significativas para la seguridad. Por consiguiente, el informe de descripción de trabajo (PRTJOBDAUT) sólo imprime descripciones de trabajos de la biblioteca especificada si la autorización de uso público para la descripción de trabajo no es *EXCLUDE *y* si la descripción de trabajo especifica un nombre de perfil de usuario en el parámetro USER.

Asimismo, cuando se imprime información sobre el subsistema (mandato PRTSBSDAUT), el sistema solamente imprime información acerca de un subsistema cuando la descripción del subsistema contiene una entrada de comunicaciones que especifica un perfil de usuario.

Si un informe determinado imprime menos información de la prevista, consulte la información de ayuda en línea para averiguar cuáles son los criterios de selección del informe.

Tabla 8. Mandatos para informes de seguridad

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
1, 40	PRTADPOBJ	Utilice el mandato Imprimir objetos que adoptan para imprimir una lista de objetos que adoptan la autorización del perfil de usuario especificado. Puede especificar un solo perfil, un nombre de perfil genérico (como por ejemplo, todos los perfiles que empiezan por Q) o todos los perfiles de usuario del sistema. Este informe tiene dos versiones. El informe completo lista todos los objetos adoptados que cumplen los criterios de selección. El informe de modificaciones lista las diferencias entre los objetos que se encuentran actualmente en el sistema y los objetos que había en el sistema la última vez que se ejecutó el informe.	QSECADPOLD[2]

Tabla 8. Mandatos para informes de seguridad (continuación)

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
2, 41	DSPAUDJRNE	Utilice el mandato Visualizar entradas de diario de auditoría para visualizar o imprimir información acerca de las entradas del diario de auditoría de seguridad. Puede seleccionar tipos de entrada específicos, usuarios específicos y un período de tiempo.	QASYxxJ4[3]
3, 42	PRTPVTAUT *AUTL	Cuando se utiliza el mandato Imprimir autorizaciones privadas para los objetos *AUTL, se recibe una lista de todas las listas de autorizaciones del sistema. El informe incluye a los usuarios que reciben autorización para cada lista así como qué clase de autorización tienen los usuarios sobre la lista. Utilice esta información para ayudarle a analizar las fuentes de la autorización de objetos en el sistema. Este informe contiene tres versiones. El informe completo contiene todas las listas de autorizaciones del sistema. El informe de modificación lista las adiciones y los cambios en la autorización desde que se ejecutó por última vez el informe. El informe de supresión lista los usuarios cuya autorización en la lista de autorizaciones se ha suprimido desde que se ejecutó por última vez el informe. Cuando se imprime el informe completo, tiene la opción de imprimir una lista de objetos que cada lista de autorizaciones protege. El sistema creará un informe por separado para cada lista de autorizaciones.	QSECATLOLD[2]
6, 45	PRTCMNSEC	Utilice el mandato Imprimir seguridad de comunicaciones para imprimir los valores relativos a la seguridad para objetos que afectan a las comunicaciones del sistema. Estos valores afectan el modo en que los usuarios y los trabajos pueden entrar en el sistema. Este mandato genera dos informes: un informe que visualiza los valores de la listas de configuraciones del sistema y un informe que lista los parámetros relativos a la seguridad para descripciones de línea, controladores y descripciones de dispositivo. Cada uno de estos informes contiene una versión completa y una modificada.	QSECCMNOLD[2]

Tabla 8. Mandatos para informes de seguridad (continuación)

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
15, 54	PRTJOBDAUT	Utilice el mandato Imprimir autorización de descripción de trabajo para imprimir una lista de descripciones de trabajos que especifican un perfil de usuario y tienen una autorización de uso público que no es *EXCLUDE. El informe muestra las autorizaciones especiales del perfil de usuario que está especificado en la descripción del trabajo. Este informe tiene dos versiones. El informe completo lista todos los objetos de descripción de trabajo que cumplen con los criterios de selección. El informe de modificaciones lista las diferencias entre los objetos de descripción de trabajo que se encuentran actualmente en el sistema y los objetos de descripción de trabajo que se encontraban en el sistema la última vez que se ejecutó el informe.	QSECJBDOLD[2]
Vea la nota 4	PRTPUBAUT	Utilice el mandato Imprimir objetos con autorización de uso público para imprimir una lista de objetos cuya autorización de uso público no es *EXCLUDE. Cuando se ejecuta el mandato, se especifica el tipo de objeto y la biblioteca o las bibliotecas del informe. Utilice el mandato PRTPUBAUT para imprimir información acerca de los objetos a los que cada usuario del sistema puede acceder. Este informe tiene dos versiones. El informe completo lista todos los objetos que cumplen los criterios de selección. El informe de modificación lista las diferencias entre los objetos especificados que se encuentran actualmente en el sistema y los objetos (del mismo tipo en la misma biblioteca) que estaban en el sistema la última vez que se ejecutó el informe.	QPBxxxxxx[5]
Vea la nota 5.	PRTPVTAUT	Utilice el mandato Imprimir autorizaciones privadas para imprimir una lista de las autorizaciones privadas sobre los objetos del tipo especificado en la biblioteca especificada. Utilice este informe para ayudarle a determinar las fuentes de autorización sobre los objetos. Este informe contiene tres versiones. El informe completo lista todos los objetos que cumplen los criterios de selección. El informe de modificación lista las diferencias entre los objetos especificados que se encuentran actualmente en el sistema y los objetos (del mismo tipo en la misma biblioteca) que estaban en el sistema la última vez que se ejecutó el informe. El informe de supresión lista los usuarios cuya autorización sobre un objeto se ha suprimido desde que se imprimió por última vez el informe.	QPVxxxxxx[5]

Tabla 8. Mandatos para informes de seguridad (continuación)

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
24, 63	PRTQAUT	Utilice el mandato Imprimir informe de colas para imprimir los valores de seguridad de las colas de salida y las colas de trabajos del sistema. Estos valores controlan quién puede visualizar y cambiar las entradas en la cola de salida o en la cola de trabajos. Este informe tiene dos versiones. El informe completo lista todos los objetos de cola de salida y de cola de trabajo que cumplen con los criterios de selección. El informe de modificaciones lista las diferencias entre los objetos de la cola de salida y de la cola de trabajo que se encuentran actualmente en el sistema y los objetos de la cola de salida y de la cola de trabajo que se encontraban en el sistema la última vez que se ejecutó el informe.	QSECQOLD[2]
25, 64	PRTSBSDAUT	Utilice el mandato Imprimir descripción de subsistema para imprimir las entradas de comunicaciones relativas a la seguridad de las descripciones de subsistema del sistema. Estos valores controlan el modo en que se puede entrar el trabajo en el sistema y cómo se ejecutan los trabajos. El informe solamente imprime una descripción de subsistema si contiene entradas de comunicaciones que especifican un nombre de perfil de usuario. Este informe tiene dos versiones. El informe completo lista todos los objetos de descripción de subsistema que cumplen con los criterios de selección. El informe de modificaciones lista las diferencias entre los objetos de descripción del subsistema y los objetos de descripción del subsistema que se encontraban en el sistema la última vez que se ejecutó el informe.	QSECSBDOLD[2]
26, 65	PRTSYSSECA	Utilice el mandato Imprimir atributos de seguridad del sistema para imprimir una lista de valores del sistema y atributos de red importantes para la seguridad. El informe muestra el valor actual y el recomendado.	
27, 66	PRTTRGPGM	Utilice el mandato Imprimir programas desencadenantes para imprimir una lista de los programas desencadenantes que están asociados con los archivos de base de datos del sistema. Este informe tiene dos versiones. El informe completo lista cada programa desencadenante que está asignado y cumple los criterios de selección. El informe de modificación lista los programas desencadenantes que se han asignado desde que se ejecutó el informe por última vez.	QSECTRGOLD[2]

Tabla 8. Mandatos para informes de seguridad (continuación)

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
28, 67	PRTUSROBJ	Utilice el mandato Imprimir objetos de usuario para imprimir una lista de los objetos de usuario (objetos no suministrados por IBM) que se encuentran en una biblioteca. Puede utilizar este informe para imprimir una lista de los objetos de usuario que están en una biblioteca (como por ejemplo, QSYS) que se encuentra en la parte del sistema de la lista de bibliotecas. Este informe tiene dos versiones. El informe completo lista todos los objetos de usuario que cumplen con los criterios de selección. El informe de modificaciones lista las diferencias entre los objetos de usuario que se encuentran actualmente en el sistema y los objetos de usuario que se encontraban en el sistema la última vez que se ejecutó el informe.	QSECPUOLD[2]
29, 68	PRTUSRPRF	Utilice el mandato Imprimir perfil de usuario para analizar los perfiles de usuario que cumplen los criterios especificados. Puede seleccionar los perfiles de usuario en función de las autorizaciones especiales, la clase de usuario o una discrepancia entre las autorizaciones especiales y la clase de usuario. Puede imprimir información de autorización, información de entorno, información de contraseña o información de nivel de contraseña.	
30, 69	PRTPRFINT	Utilice el mandato Imprimir información interna de perfil para imprimir un informe de la información interna sobre el número de entradas.	
31, 70	CHKOBJITG	Utilice el mandato Comprobar integridad de objetos para determinar si los objetos operativos (como por ejemplo, los programas) se han cambiado sin utilizar un compilador. Este mandato le puede ayudar a detectar intentos de introducir un programa de virus en el sistema o de cambiar un programa para seguir instrucciones no autorizadas. La publicación *iSeries Security Reference* proporciona más información acerca del mandato CHKOBJITG.	

Tabla 8. Mandatos para informes de seguridad (continuación)

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado

Notas:

1. Las opciones pertenecen al menú SECBATCH.
2. Este archivo está en la biblioteca QUSRSYS.
3. xx es el tipo de entrada de diario de dos caracteres. Por ejemplo, el archivo de salida modelo para las entradas de diario AE es QSYS/QASYAEJ4. Los archivos de salida del modelo se describen en el Apéndice F del manual *iSeries Security Reference*.
4. El menú SECBATCH contiene opciones para los tipos de objetos que normalmente conciernen a los administradores de seguridad. Por ejemplo, utilice las opciones 11 o 50 para ejecutar el mandato PRTPUBAUT en los objetos tipo *FILE. Utilice las opciones generales (18 y 57) para especificar el tipo de objeto.
5. El menú SECBATCH contiene opciones para los tipos de objetos que normalmente conciernen a los administradores de seguridad. Por ejemplo, las opciones 12 o 51 ejecutan el mandato PRTPVTAUT en los archivos tipo *FILE. Utilice las opciones generales (19 y 58) para especificar el tipo de objeto.
6. xxxxxx en el nombre del archivo es el tipo de objeto. Por ejemplo, el archivo de los objetos de programa recibe el nombre de QPBPGM para las autorizaciones de uso público y QPVPGM para las autorizaciones privadas. Los archivos están en la biblioteca QUSRSYS.

   El archivo contiene un miembro para cada biblioteca para la que se ha impreso el informe. El nombre de miembro es el mismo que el nombre de biblioteca.

Mandatos para personalizar la seguridad

La Tabla 9 describe los mandatos que puede utilizar para personalizar la seguridad en su sistema. Estos mandatos se encuentran en el menú SECTOOLS.

Tabla 9. Mandatos para personalizar el sistema

Opción de menú[1]	Nombre de mandato	Descripción	Archivo de base de datos utilizado
60	CFGSYSSEC	Utilice el mandato Configurar seguridad del sistema para establecer los valores del sistema relativos a la seguridad en sus valores recomendados. El mandato también establece la auditoría de seguridad en el sistema. El apartado "Valores establecidos por el mandato Configurar seguridad del sistema" en la página 42 describe las acciones del mandato. **Nota:** Para obtener recomendaciones sobre seguridad personalizadas para su situación concreta, ejecute el Asistente de seguridad de iSeries o el Asesor de seguridad de iSeries en lugar de ejecutar este mandato. Vea el Capítulo 2, "Asistente de seguridad de iSeries y Planificador de seguridad de eServer", en la página 11 para obtener información sobre estas herramientas.	
61	RVKPUBAUT	Utilice el mandato Revocar autorización de uso público para establecer la autorización de uso público en *EXCLUDE para un conjunto de mandatos relativos a la seguridad en el sistema. El apartado "Funciones del mandato Revocar autorización de uso público" en la página 44 lista las acciones que el mandato RVKPUBAUT lleva a cabo.	

Notas:

1. Las opciones pertenecen al menú SECTOOLS.

Valores establecidos por el mandato Configurar seguridad del sistema

La Tabla 10 lista los valores del sistema que se establecen al ejecutar el mandato CFGSYSSEC. El mandato CFGSYSSEC ejecuta un programa que se denomina QSYS/QSECCFGS.

Tabla 10. Valores establecidos por el mandato CFGSYSSEC

Nombre del valor del sistema	Valor	Descripción del valor del sistema
QALWOBJRST	*NONE	Si se pueden restaurar los programas de estado del sistema y los programas que adoptan autorización
QAUTOCFG	0 (No)	Configuración automática de nuevos dispositivos
QAUTOVRT	0	Número de descripciones de dispositivos virtuales que el sistema creará automáticamente si no hay ningún dispositivo disponible para su utilización
QDEVRCYACN	*DSCMSG (Desconectar con mensaje)	Acción del sistema cuando se restablecen las comunicaciones
QDSCJOBITV	120	Período de tiempo antes de que el sistema emprenda una acción en un trabajo desconectado
QDSPSGNINF	1 (Sí)	Si los usuarios visualizan la pantalla de información de inicio de sesión
QINACTITV	60	Período de tiempo antes de que el sistema emprenda una acción en un trabajo interactivo inactivo
QINACTMSGQ	*ENDJOB	Acción que el sistema emprende para un trabajo inactivo
QLMTDEVSSN	1 (Sí)	Si los usuarios se ven limitados a iniciar la sesión en un dispositivo cada vez
QLMTSECOFR	1 (Sí)	Si los usuarios *ALLOBJ y *SERVICE tienen como límites los dispositivos especificados
QMAXSIGN	3	Cuántos intentos de inicio de sesión consecutivos e insatisfactorios se permiten
QMAXSGNACN	3 (Ambos)	Si el sistema inhabilita la estación de trabajo o el perfil de usuario cuando se alcanza el límite QMAXSIGN
QRMTSIGN	*FRCSIGNON	Cómo maneja el sistema un intento de inicio de sesión remoto (paso a través o TELNET).
QRMTSVRATR	0 (Desactivar)	Permite analizar remotamente el sistema.
QSECURITY [1 en la página 43]	50	El nivel de seguridad que se aplica
QVFYOBJRST	3 (Verificar firmas al restaurar)	Verificar objeto al restaurar
QPWDEXPITV	60	Con qué frecuencia los usuarios deben cambiar sus contraseñas
QPWDMINLEN	6	Longitud mínima de las contraseñas
QPWDMAXLEN	8	Longitud máxima de las contraseñas
QPWDPOSDIF	1 (Sí)	Si cada posición en una contraseña nueva debe ser diferente de la misma posición en la última contraseña
QPWDLMTCHR	Vea la nota 2 en la página 43	Caracteres que no se permiten en las contraseñas
QPWDLMTAJC	1 (Sí)	Si los números adyacentes están prohibidos en las contraseñas
QPWDLMTREP	2 (No se puede repetir consecutivamente)	Si los caracteres repetidos están prohibidos en las contraseñas

Tabla 10. Valores establecidos por el mandato CFGSYSSEC (continuación)

Nombre del valor del sistema	Valor	Descripción del valor del sistema
QPWDRQDDGT	1 (Sí)	Si las contraseñas deben tener como mínimo un número
QPWDRQDDIF	1 (32 contraseñas exclusivas)	Cuántas contraseñas exclusivas se necesitan antes de que se pueda repetir una contraseña
QPWDVLDPGM	*NONE	El programa de salida de usuario que el sistema invoca antes de validar las contraseñas

Notas:

1. Si actualmente está ejecutando con un valor QSECURITY de 40 o inferior, asegúrese de revisar la información del Capítulo 2 de la publicación *iSeries Security Reference* antes de cambiar a un nivel de seguridad superior.
2. Los caracteres restringidos se almacenan en el ID de mensaje CPXB302 del archivo de mensajes QSYS/QCPFMSG. Se entregan como AEIOU@$#. Puede utilizar el mandato Cambiar descripción de mensaje (CHGMSGD) para cambiar los caracteres restringidos. El valor del sistema QPWDLMTCHR no se aplica en los niveles de contraseña 2 ó 3.

El mandato CFGSYSSEC también establece la contraseña en *NONE para los siguientes perfiles de usuario suministrados por IBM:

QSYSOPR

QPGMR

QUSER

QSRV

QSRVBAS

Por último, el mandato CFGSYSSEC define la auditoría de seguridad mediante el mandato Cambiar auditoría de seguridad (CHGSECAUD). El mandato CFGSYSSEC activa la auditoría de acción y objeto, además especifica el conjunto de acciones que se auditarán por omisión en el mandato CHGSECAUD.

Personalización del programa

Si algunos de estos valores no son adecuados para su instalación, puede crear su propia versión del programa que procese el mandato. Haga lo siguiente:

__ Paso 1. Utilice el mandato Recuperar fuente CL (RTVCLSRC) para copiar la fuente para el programa que se ejecuta al utilizar el mandato CFGSYSSEC. El programa que se recupera es QSYS/QSECCFGS. Cuando lo recupere, déle un *nombre distinto*.

__ Paso 2. Edite el programa y efectúe las modificaciones. A continuación, compílelo. Cuando lo compile, asegúrese de que *no* sustituye el programa QSYS/QSECCFGS suministrado por IBM.Su programa deberá tener otro nombre.

__ Paso 3. Utilice el mandato Cambiar mandato (CHGCMD) para cambiar el programa de modo que procese el parámetro de procesar mandato (PGM) para el mandato CFGSYSSEC. Establezca el valor PGM con el nombre de su programa. Por ejemplo, si crea un programa en la biblioteca QGPL que se denomina MYSECCFG, deberá escribir lo siguiente:

```
CHGCMD CMD(QSYS/CFGSYSSEC) PGM(QGPL/MYSECCFG)
```

Nota: Si modifica el programa QSYS/QSECCFGS, IBM no puede garantizar ni dar por supuesto su fiabilidad, mantenimiento,

rendimiento o funcionamiento. Las garantías implícitas de comercialización e idoneidad para una finalidad determinada están excluidas expresamente.

Funciones del mandato Revocar autorización de uso público

Puede utilizar el mandato Revocar autorización de uso público (RVKPUBAUT) para establecer la autorización de uso público en *EXCLUDE para un conjunto de mandatos y programas. El mandato RVKPUBAUT ejecuta un programa que se denomina QSYS/QSECRVKP. Tal como se entrega, el programa QSECRVKP revoca la autorización de uso público (estableciendo la autorización de uso público en *EXCLUDE) para los mandatos que aparecen listados en la Tabla 11 y las interfaces de programación de aplicaciones (API) que aparecen listadas en la Tabla 12. Cuando se recibe el sistema, estos mandatos y estas API tienen la autorización de uso público establecida en *USE.

Los mandatos que aparecen listados en la Tabla 11 y las API listadas en la Tabla 12 realizan funciones en el sistema que pueden permitir que se realicen acciones no permitidas. Como administrador de seguridad, debe autorizar explícitamente a los usuarios para que ejecuten estos mandatos y programas en lugar de ponerlos a disposición de todos los usuarios del sistema.

Si ejecuta el mandato RVKPUBAUT, especifique la biblioteca que contiene los mandatos. El valor por omisión es la biblioteca QSYS. Si dispone de más de un idioma nacional en el sistema, debe ejecutar el mandato para cada biblioteca QSYSxxx.

Tabla 11. Mandatos cuya autorización de uso público se establece con el mandato RVKPUBAUT

ADDAJE	CHGJOBQE	RMVCMNE
ADDCFGLE	CHGPJE	RMVJOBQE
ADDCMNE	CHGRTGE	RMVPJE
ADDJOBQE	CHGSBSD	RMVRTGE
ADDPJE	CHGWSE	RMVWSE
ADDRTGE	CPYCFGL	RSTLIB
ADDWSE	CRTCFGL	RSTOBJ
CHGAJE	CRTCTLAPPC	RSTS36F
CHGCFGL	CRTDEVAPPC	RSTS36FLR
CHGCFGLE	CRTSBSD	RSTS36LIBM
CHGCMNE	ENDRMTSPT	STRRMTSPT
CHGCTLAPPC	RMVAJE	STRSBS
CHGDEVAPPC	RMVCFGLE	WRKCFGL

Las API de la Tabla 12 se encuentran todas en la biblioteca QSYS:

Tabla 12. Programas cuya autorización de uso público se establece con el mandato RVKPUBAUT

QTIENDSUP
QTISTRSUP
QWTCTLTR
QWTSETTR
QY2FTML

Al ejecutar el mandato RVKPUBAUT, el sistema establece autorización de uso público en *USE para el directorio raíz (a menos que ya sea *USE o inferior).

Personalización del programa

Si algunos de estos valores no son adecuados para su instalación, puede crear su propia versión del programa que procesa el mandato. Haga lo siguiente:

__ Paso 1. Utilice el mandato Recuperar fuente CL (RTVCLSRC) para copiar el fuente del programa que se ejecuta al utilizar el mandato RVKPUBAUT. El programa que se recupera es QSYS/QSECRVKP. Cuando lo recupere, déle un *nombre distinto*.

__ Paso 2. Edite el programa y efectúe las modificaciones. A continuación, compílelo. Cuando lo compile, asegúrese de que *no* sustituye el programa QSYS/QSECRVKP suministrado por IBM. Su programa deberá tener otro nombre.

__ Paso 3. Utilice el mandato Cambiar mandato (CHGCMD) para cambiar el programa de modo que procese el parámetro de procesar mandato (PGM) para el mandato RVKPUBAUT. Establezca el valor PGM con el nombre de su programa. Por ejemplo, si crea un programa en la biblioteca QGPL que se denomina MYRVKPGM, deberá escribir lo siguiente:

```
CHGCMD CMD(QSYS/RVKPUBAUT) PGM(QGPL/MYRVKPGM)
```

Nota: Si modifica el programa QSYS/QSECRVKP, IBM no puede garantizar ni dar por supuesto su fiabilidad, mantenimiento, rendimiento o función. Las garantías implícitas de comercialización e idoneidad para una finalidad determinada están excluidas expresamente.

Parte 2. Seguridad avanzada de iSeries

Capítulo 5. Protección de la información con la autorización sobre objetos

El reto de un administrador de seguridad es proteger la información de la organización sin contrariar a los usuarios del sistema. Debe asegurarse de que los usuarios tengan autorización suficiente para realizar los trabajos sin tener que otorgarles una autorización que les permita examinar el sistema y hacer cambios no autorizados.

Consejo de seguridad

Las autorizaciones demasiado estrictas pueden dar un mal resultado. Frente a restricciones demasiado estrictas en las autorizaciones los usuarios reaccionan a veces compartiendo contraseñas entre ellos.

El sistema operativo OS/400 proporciona seguridad de objetos integrada. Los usuarios deben utilizar las interfaces que proporciona el sistema para acceder a los objetos. Por ejemplo, si quiere acceder a un archivo de base de datos, debe utilizar mandatos o programas pensados para acceder a archivos de base de datos. No puede utilizar un mandato destinado a acceder a una cola de mensajes o a unas anotaciones de trabajo.

Siempre que se utiliza una interfaz del sistema para acceder a un objeto, el sistema verifica si tiene autoridad sobre el objeto requerido por la interfaz. La autorización sobre objetos es una herramienta poderosa y flexible para proteger las partidas del sistema. El reto de un administrador de seguridad es establecer un esquema de seguridad de objetos efectivo que pueda gestionar y mantener.

Imposición de la autorización sobre objetos

Siempre que se intenta acceder a un objeto, el sistema operativo comprueba la autorización que se tiene sobre el objeto. Sin embargo, si el nivel de seguridad del sistema (valor del sistema QSECURITY) se establece en 10 ó 20, todos los usuarios están automáticamente autorizados para acceder a todos los objetos ya que todos los perfiles de usuario tienen autorización especial *ALLOBJ.

Consejo acerca de la autorización sobre objetos: Si no está seguro de que está utilizando la autorización sobre objetos, compruebe el valor del sistema QSECURITY (nivel de seguridad). Si QSECURITY es 10 ó 20, no está utilizando la seguridad sobre objetos.

Debe realizar una planificación y una preparación antes de cambiar a un nivel de seguridad 30 o superior. De lo contrario, los usuarios no serán capaces de acceder a la información necesaria.

El tema **Seguridad y planificación básica del sistema** de Information Center proporciona un método para analizar sus aplicaciones y decidir cómo configurará la seguridad sobre objetos. Si aún no está utilizando la seguridad sobre objetos o si su esquema de seguridad sobre objetos se ha quedado anticuado, lea este tema como iniciación.

Seguridad de los menús

El servidor iSeries estaba diseñado originariamente como un producto de continuación del S/36 y del S/38. Muchas instalaciones de servidores iSeries eran anteriormente instalaciones de S/36 o instalaciones de S/38. Para controlar lo que los usuarios podían hacer, los administradores de seguridad de los primeros sistemas utilizaban a menudo una técnica llamada **seguridad de menús** o **control de acceso a menús**.

El control de acceso a menús significa que cuando un usuario inicia la sesión, el usuario ve un menú. El usuario puede realizar solamente las funciones que están en el menú. El usuario no puede acceder a una línea de mandatos del sistema para llevar a cabo funciones que no estén en el menú. En teoría, el administrador de seguridad no tiene que preocuparse de la autorización sobre los objetos ya que los menús y los programas controlan lo que pueden hacer los usuarios.

El servidor iSeries proporciona diversas opciones de perfil de usuario como ayuda para el control de acceso a menús; puede utilizar:

- El parámetro **Menú inicial** (INLMNU) para controlar qué menú verá primero el usuario tras iniciar la sesión.
- El parámetro **Programa inicial** (INLPGM) para ejecutar un programa de configuración antes de que el usuario vea un menú. O bien puede utilizar el parámetro INLPGM para restringir a un usuario a la utilización de un único programa.
- El parámetro **Limitar posibilidades** (LMTCPB) para restringir a un usuario a un conjunto limitado de mandatos. También evita que el usuario especifique un programa o menú inicial distinto en la pantalla Inicio de sesión. (El parámetro LMTCPB sólo limita mandatos entrados desde la línea de mandatos).

Limitaciones del control de acceso a menús

Los sistemas informáticos y los usuarios de sistemas informáticos han cambiado mucho en los últimos años. Se dispone de muchas herramientas tales como programas de consulta y hojas de cálculo, de forma que los usuarios pueden programar por su cuenta para quitar carga de trabajo a los departamentos de desarrollo de software. Algunas herramientas, tales como SQL o ODBC, proporcionan la posibilidad de ver y cambiar información. Habilitar estas herramientas dentro de una estructura de menús es muy difícil.

Las estaciones de trabajo de función fija (“pantalla verde”) se están sustituyendo rápidamente por PC y redes de sistema a sistema. Si el sistema forma parte de una red, los usuarios pueden entrar en él sin haber visto nunca una pantalla de inicio de sesión o un menú.

El administrador de seguridad que intenta imponer el control de acceso a menús se encuentra con dos problemas fundamentales:

- Si se tiene éxito en la limitación de menús para los usuarios, estos estarán probablemente descontentos porque su capacidad de utilizar herramientas modernas estará limitada.
- Si no se tiene éxito, se estará poniendo en peligro información confidencial de gran importancia que el control de acceso a menús debería proteger. Cuando el sistema participa en una red, la capacidad de imponer el control de acceso a menús disminuye. Por ejemplo, el parámetro LMTCPB se aplica sólo a los mandatos que se entran desde una línea de mandatos de una sesión interactiva. El parámetro LMTCPB no afecta a las peticiones de sesiones de comunicación, tales como la transferencia de archivos de PC, FTP o los mandatos remotos.

Mejora del control de acceso a menús con la seguridad de objetos

Con las numerosas opciones nuevas disponibles para conectarse a sistemas, un esquema de seguridad del servidor iSeries viable para el futuro no puede basarse únicamente en el control de acceso a menús. En este tema se proporcionan sugerencias para avanzar hacia un entorno de seguridad que complemente el control de acceso a menús.

El tema *Seguridad básica del sistema y planificación* del Information Center describe una técnica para analizar la autorización que los usuarios deben tener sobre los objetos para ejecutar las aplicaciones actuales. Asigne los usuarios a los grupos y dé a los grupos la autorización adecuada. Este acercamiento es razonable y lógico. Sin embargo, si el sistema ha estado funcionando durante muchos años y tiene muchas aplicaciones, la tarea de analizar las aplicaciones y configurar las autorizaciones sobre objetos parece excesiva.

Consejo de autorización sobre objetos: Sus menús actuales combinados con programas que adoptan la autorización de los propietarios de los programas pueden proporcionar un paso más allá del control de acceso a menús. Asegúrese de proteger tanto los programas que adoptan autorización como los perfiles de usuario que los poseen.

Probablemente será capaz de utilizar los menús actuales como ayuda para configurar un entorno de transición mientras se analizan gradualmente las aplicaciones y los objetos. A continuación se muestra un ejemplo que utiliza el menú Entrada de pedidos (OEMENU) y los archivos y programas asociados al mismo.

Ejemplo: Puesta a punto de un entorno de transición

Este ejemplo empieza con las suposiciones y los requisitos siguientes:

- Todos los archivos están en la biblioteca ORDERLIB.
- No conoce los nombres de todos los archivos. Tampoco sabe qué autorización necesitan las opciones de menú para los distintos archivos.
- El menú y los programas que llama están en una biblioteca llamada ORDERPGM.
- Quiere que todos los que puedan iniciar la sesión en el sistema sean capaces de ver información en todos los archivos de pedidos, archivos de clientes y archivos de artículos (con consultas u hojas de cálculo, por ejemplo).
- Sólo los usuarios cuyo menú de inicio de sesión sea el menú OEMENU deben tener capacidad para cambiar los archivos. Y, para hacerlo, deben utilizar los programas del menú.
- Los usuarios del sistema que no son administradores de seguridad no tienen autorización especial *ALLOBJ o *SECADM.

Siga los pasos siguientes para cambiar este entorno de control de acceso a menús para ajustarse a la necesidad de consultas:

__ Paso 1. Haga una lista de los usuarios cuyo menú inicial sea OEMENU.

Puede utilizar el mandato Imprimir perfil de usuario (PRTUSRPRF *ENVINFO) para listar el entorno de cada perfil de usuario del sistema. El informe incluye el menú inicial, el programa inicial y la biblioteca actual. La Figura 7 en la página 68 muestra un ejemplo del informe.

__ Paso 2. Asegúrese de que el objeto OEMENU (puede ser un objeto *PGM o un objeto *MENU) es propiedad de un perfil de usuario que no se utiliza para el inicio de sesión. El perfil de usuario debe inhabilitarse o tener una contraseña *NONE. Para este ejemplo suponga que OEOWNER posee el objeto de programa OEMENU.

__ Paso 3. Asegúrese de que el perfil de usuario que posee el programa OEMENU no es un perfil de grupo. Puede utilizar el mandato siguiente:

```
DSPUSRPRF USRPRF(OEOWNER) TYPE(*GRPMBR)
```

__ Paso 4. Cambie el programa OEMENU para adoptar la autorización del perfil de usuario OEOWNER. (Utilice el mandato CHGPGM para cambiar el parámetro USRPRF por *OWNER.)

Nota: Los objetos *MENU no pueden adoptar autorización. Si OEMENU es un objeto *MENU, puede adaptar este ejemplo llevando a cabo una de las acciones siguientes:

- Cree un programa para visualizar el menú.
- Utilice la autorización adoptada para los programas que se ejecutan cuando el usuario selecciona opciones del menú OEMENU.

__ Paso 5. Establezca la autorización de uso público de todos los archivos de ORDERLIB en *USE tecleando los dos mandatos siguientes:

```
RVKOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
    AUT(*ALL)
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(*PUBLIC)
    AUT(*USE)
```

Recuerde que si selecciona la autorización *USE, los usuarios pueden copiar el archivo utilizando la transferencia de archivos de PC o FTP.

__ Paso 6. Proporcione autorización *ALL sobre los archivos al perfil que posee el programa tecleando lo siguiente:

```
GRTOBJAUT OBJ(ORDERLIB/*ALL) OBJTYPE(*FILE) USER(OEOWNER)
    AUT(*ALL)
```

Para la mayoría de las aplicaciones es suficiente la autorización *CHANGE sobre los archivos. Sin embargo, las aplicaciones pueden realizar funciones, tales como borrar archivos físicos, que necesitan una autorización superior a *CHANGE. Es posible que deba analizar las aplicaciones y proporcionar sólo la autorización mínima necesaria para cada aplicación. Sin embargo, durante el período de transición, adoptando la autorización *ALL, se evitan anomalías en las aplicaciones que puedan deberse a una autorización insuficiente.

__ Paso 7. Restrinja la autorización para los programas de la biblioteca de pedidos tecleando lo siguiente:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(*PUBLIC)
    AUT(*EXCLUDE)
```

__ Paso 8. Otorgue al perfil OEOWNER autorización sobre los programas de la biblioteca tecleando lo siguiente:

```
GRTOBJAUT OBJ(ORDERPGM/*ALL) OBJTYPE(*PGM) USER(OEOWNER)
    AUT(*USE)
```

__ Paso 9. Otorgue a los usuarios identificados en el paso 1 autorización sobre el programa de menú tecleando lo siguiente para cada usuario:

```
GRTOBJAUT OBJ(ORDERPGM/OEMENU) OBJTYPE(*PGM)
     USER(nombre-perfil-usuario) AUT(*USE)
```

Cuando haya terminado estos pasos, todos los usuarios del sistema que no se hayan excluido explícitamente serán capaces de acceder (pero no de cambiar) a los archivos de la biblioteca ORDERLIB. Los usuarios con autorización sobre el programa OEMENU tendrán capacidad de utilizar los programas que están en el menú para actualizar archivos de la biblioteca ORDERLIB. Sólo los usuarios que tengan autorización sobre el programa OEMENU serán capaces de cambiar los archivos de esta biblioteca. Una combinación de seguridad de objetos y control de acceso a menú protege los archivos.

Al completar pasos similares para todas las bibliotecas que contienen datos de usuario, se habrá creado un esquema simple para controlar las actualizaciones de base de datos. Este método evita que los usuarios del sistema actualicen archivos de base de datos, excepto cuando utilicen los menús y programas aprobados. Al mismo tiempo, los archivos de base de datos quedan disponibles para que los usuarios los vean, los analicen y los copien mediante herramientas de soporte de decisiones o mediante enlaces desde otro sistema o desde un PC.

Consejo de autorización sobre objetos: Cuando el sistema participa en una red, la autorización *USE puede proporcionar más autorización de la esperada. Por ejemplo, con FTP, puede hacer una copia de un archivo en otro sistema (incluyendo un PC) si tiene autorización *USE sobre el archivo.

Utilización de la seguridad de bibliotecas para complementar la seguridad por menús

Para acceder a un objeto de biblioteca debe tener autorización sobre el objeto y sobre la biblioteca. La mayoría de las operaciones necesitan la autorización *EXECUTE o la autorización *USE sobre la biblioteca.

Dependiendo de la situación, puede ser capaz de utilizar la autorización de biblioteca como una manera simple de asegurar objetos. Por ejemplo, suponga que en el ejemplo del menú de Entrada de pedidos, todos los que tengan autorización sobre el menú de Entrada de pedidos puedan utilizar todos los programas de la biblioteca ORDERPGM. En lugar de asegurar los programas individuales, puede establecer la autorización de uso público sobre la biblioteca ORDERPGM en *EXCLUDE. Puede otorgar entonces autorización *USE sobre la biblioteca a perfiles de usuario específicos, lo que les permitirá utilizar los programas de la biblioteca. (Esto da por supuesto que la autorización de uso público para los programas es *USE o mayor).

La autorización sobre bibliotecas puede ser un método simple y eficiente de administrar la autorización sobre objetos. Sin embargo debe asegurarse de que conoce el contenido de las bibliotecas que se aseguran de forma que no proporcione acceso no intencionado a los objetos.

Configuración de la propiedad de objetos

La propiedad de objetos en el sistema es una parte importante del esquema de autorización sobre objetos. Por omisión, el propietario de un objeto tiene autorización *ALL sobre el objeto. El capítulo 5 de la publicación *iSeries Security Reference* proporciona recomendaciones y ejemplos para planificar la propiedad de los objetos. A continuación se proporcionan algunos consejos:

- Por lo general, los perfiles de grupo no deben ser propietarios de objetos. Si un perfil de grupo posee un objeto, todos los miembros del grupo tendrán autorización *ALL sobre el objeto a menos que el miembro del grupo esté excluido de forma explícita.

- Si utiliza la autorización adoptada, considere si los perfiles de usuario de los propios programas deben poseer también objetos de aplicación tales como archivos. Probablemente no querrá que los usuarios que ejecutan los programas que adoptan autorización tengan autorización *ALL sobre los archivos.

Si está utilizando iSeries Navigator, lo conseguirá completando los cambios utilizando la función de **políticas** de seguridad. Para obtener más información, consulte el iSeries Information Center (vea "Requisitos e información relacionada" en la página xii para conocer más detalles).

Autorización sobre objetos para mandatos del sistema y programas

A continuación se proporcionan varias sugerencias para cuando se restringe la autorización a los objetos proporcionados por IBM:

- Cuando se tiene más de un idioma nacional en el sistema, el sistema tiene más de una biblioteca del sistema (QSYS). El sistema tiene una biblioteca QSYSxxxx para cada idioma nacional del sistema. Si va a utilizar la autorización sobre objetos para controlar los mandatos del sistema, acuérdese de asegurar el mandato en la biblioteca QSYS y en todas las bibliotecas QSYSxxx del sistema.
- La biblioteca del System/38 proporciona a veces un mandato cuya función es equivalente a los mandatos que quiere restringir. Asegúrese de restringir el mandato equivalente en la biblioteca QSYS38.
- Si tiene el entorno System/36, puede necesitar restringir programas adicionales. Por ejemplo, el programa QY2FTML proporciona transferencia de archivos del System/36.

Auditoría de funciones de seguridad

Este capítulo describe técnicas para realizar una auditoría de la eficacia de la seguridad en su sistema. Los motivos para realizar una auditoría de la seguridad del sistema pueden ser diversos:

- Para evaluar si el plan de seguridad es completo.
- Para asegurarse de que los controles de seguridad planificados están en funcionamiento. Este tipo de auditoría suele realizarla el responsable de seguridad como parte de la administración diaria de la seguridad. También se lleva a cabo, a veces más detalladamente, como parte de una revisión periódica de la seguridad por parte de auditores internos o externos.
- Para asegurarse de que la seguridad del sistema sigue el ritmo de los cambios que se realizan en el entorno del sistema. Estos son algunos ejemplos de los cambios que afectan a la seguridad:
  - Objetos nuevos creados por usuarios del sistema
  - Usuarios nuevos admitidos en el sistema
  - Cambio de la propiedad de objetos (autorización no ajustada)
  - Cambio de responsabilidades (grupo de usuarios modificado)
  - Autorización temporal (no revocada a tiempo)
  - Instalación de nuevos productos
- Para prepararse para un evento futuro como, por ejemplo, instalar una nueva aplicación, ir a un nivel de seguridad superior o configurar una red de comunicaciones.

Las técnicas descritas en este capítulo son apropiadas para todas esas situaciones. Los elementos para los que realice la auditoría y la frecuencia con que lo haga dependerán del tamaño y de las necesidades de seguridad de su organización. La

finalidad de este capítulo es averiguar qué información hay disponible, cómo obtenerla y por qué es necesaria, en lugar de ofrecer directrices sobre la frecuencia de las auditorías.

Este apartado consta de tres partes:

- Una lista de comprobación de los elementos de seguridad que pueden planificarse y auditarse.
- Información sobre la puesta a punto y la utilización del diario de auditoría proporcionado por el sistema.
- Otras técnicas disponibles para reunir información sobre seguridad en el sistema.

La auditoría de seguridad implica el uso de mandatos en el sistema iSeries y el acceso a información de anotaciones y diarios en el sistema. Puede interesarle crear un perfil especial para que lo utilice quien tenga que realizar una auditoría de seguridad de su sistema. El perfil del auditor necesitará la autorización especial *AUDIT para poder modificar las características de auditoría de su sistema. Algunas de las tareas de auditoría sugeridas en este capítulo requieren un perfil de usuario con la autorización especial *ALLOBJ y *SECADM. Asegúrese de establecer la contraseña para el perfil de auditor como *NONE al finalizar el periodo de auditoría.

Para obtener más detalles sobre la auditoría de seguridad vea el capítulo 9 de la publicación *Seguridad, Manual de consulta*.

Análisis de perfiles de usuario

Puede visualizar o imprimir una lista completa de todos los usuarios del sistema con el mandato Visualizar usuarios autorizados (DSPAUTUSR). La lista puede ordenarse por nombre de perfil o nombre de perfil de grupo. A continuación se proporciona un ejemplo del orden del perfil de grupo:

```
                        Visualizar usuarios autorizados

Perfil      Perfil      Último   Sin
Grupo       usuario     cambio   contraseña Texto
DPTSM                   contraseña
            ANDERSOR    08/04/0x            Roger Anders
            VINCENTM    09/15/0x            Mark Vincent
DPTWH
            ANDERSOR    08/04/0x            Roger Anders
            WAGNERR     09/06/0x            Rose Wagner
QSECOFR           JONESS      09/20/0x            Sharon Jones
            HARRISOK    08/29/0x            Ken Harrison
*NO GROUP
            DPTSM       09/05/0x    X       Ventas y Marketing
            DPTWH       08/13/0x    X       Almacén
            RICHARDS    09/05/0x            Janet Richards
            SMITHJ      09/18/0x            John Smith
```

Imprimir perfiles de usuario seleccionados

Puede utilizar el mandato Visualizar perfil de usuario (DSPUSRPRF) para crear un archivo de salida, que puede procesar utilizando una herramienta de consulta.

```
DSPUSRPRF USRPRF(*ALL) +
          TYPE(*BASIC) OUTPUT(*OUTFILE)
```

Puede utilizar una herramienta de consulta para crear diversos informes de análisis de su archivo de salida, por ejemplo:

- Una lista de todos los usuarios que tienen las autorizaciones especiales *ALLOBJ y *SPLCTL.
- Una lista de todos los usuarios ordenados por un campo de perfil de usuario, por ejemplo programa inicial o clase de usuario.

Puede crear programas de consulta para generar distintos informes del archivo de salida. Por ejemplo:

- Listar todos los perfiles de usuarios que tengan autorizaciones especiales, seleccionando registros en los que el campo UPSPAU no sea *NONE.
- Listar todos los usuarios a los que les esté permitido entrar mandatos, seleccionando registros en los que el campo *Limitar posibilidades* (denominado UPLTCP en el archivo de salida de base de datos modelo) sea *NO o *PARTIAL.
- Listar todos los usuarios que tengan un menú inicial o programa inicial concreto.
- Listar los usuarios inactivos fijándose en el campo de fecha de último inicio de sesión.

Examen de perfiles de usuario de gran tamaño

Los perfiles de usuario con un gran número de autorizaciones, que parecen estar repartidos por el sistema al azar, pueden reflejar una falta de planificación de la seguridad. A continuación se muestra un método para localizar los perfiles de usuario de gran tamaño y cómo evaluarlos:

1. Utilice el mandato Visualizar descripción de objeto (DSPOBJD) para crear un archivo de salida que contenga información sobre todos los perfiles de usuario del sistema:

   ```
   DSPOBJD OBJ(*ALL) OBJTYPE(*USRPRF) +
           DETAIL(*BASIC) OUTPUT(*OUTFILE)
   ```

2. Cree un programa de consulta para listar el nombre y el tamaño de cada perfil de usuario, en secuencia descendente por su tamaño.
3. Imprima información detallada sobre los perfiles de usuario más grandes y evalúe las autorizaciones y los objetos que poseen para ver si son los apropiados:

   ```
   DSPUSRPRF USRPRF(nombre-perfil-usuario) +
             TYPE(*OBJAUT) OUTPUT(*PRINT)
   DSPUSRPRF USRPRF(nombre-perfil-usuario) +
             TYPE(*OBJOWN) OUTPUT(*PRINT)
   ```

   Algunos perfiles de usuario suministrados por IBM son de gran tamaño debido al número de objetos que poseen. No suele ser necesario listarlos y analizarlos. No obstante, deberá comprobar si hay programas que adoptan la autorización de los perfiles de usuario suministrados por IBM que tengan la autorización especial *ALLOBJ, por ejemplo QSECOFR y QSYS.

Para obtener más detalles sobre la auditoría de seguridad vea el capítulo 9 de la publicación *Seguridad, Manual de consulta*.

Análisis de autorizaciones sobre objetos

Puede utilizar el siguiente método para determinar quién tiene autorización sobre las bibliotecas del sistema:

1. Utilice el mandato DSPOBJD para listar todas las bibliotecas del sistema:

   ```
   DSPOBJD OBJ(QSYS/*ALL) OBJTYPE(*LIB) ASPDEV(*ALLAVL) OUTPUT(*PRINT)
   ```

Nota: Este mandato no mostrará las bibliotecas de agrupaciones de almacenamiento auxiliar independientes que no están en estado DISPONIBLE.

2. Utilice el mandato Visualizar autorización sobre objeto (DSPOBJAUT) para listar las autorizaciones sobre una biblioteca específica:

```
DSPOBJAUT OBJ(QSYS/nombre-biblioteca) OBJTYPE(*LIB) +
          ASPDEV(nombre-dispositivo-asp) OUTPUT(*PRINT)
```

3. Utilice el mandato Visualizar biblioteca (DSPLIB) para listar los objetos de la biblioteca:

```
DSPLIB LIB(QSYS/nombre-biblioteca) ASPDEV(nombre-dispositivo-asp) OUTPUT(*PRINT)
```

Utilizando estos informes, puede determinar qué hay en una biblioteca y quién tiene acceso a la misma. Si es necesario, puede utilizar el mandato DSPOBJAUT para ver también la autorización para objetos seleccionados de la biblioteca.

Búsqueda de objetos alterados

Puede utilizar el mandato Comprobar integridad de objetos (CHKOBJITG) para buscar objetos que hayan sido alterados. Un objeto alterado suele ser una indicación de que alguien intenta entrar en su sistema. Puede interesarle ejecutar este mandato después de que alguien haya realizado alguna de las siguientes acciones:

- Restaurar programas al sistema
- Utilizar herramientas de servicio dedicado (DST)

Cuando ejecute el mandato, el sistema creará un archivo de base de datos que contendrá información sobre cualquier posible problema de integridad. Puede comprobar los objetos propiedad de un perfil, de varios perfiles distintos o de todos los perfiles. Puede buscar objetos cuyo dominio haya sido alterado. También puede volver a calcular los valores de validación de programas para buscar objetos de los tipos *PGM, *SRVPGM, *MODULE y *SQLPKG que se hayan alterado.

Para ejecutar el programa CHKOBJITG es necesaria la autorización especial *AUDIT. El mandato puede tardar en ejecutarse debido a las exploraciones y cálculos que realiza. Deberá ejecutarlo en un momento en que el sistema no esté muy ocupado.

Nota: Los perfiles que poseen muchos objetos con muchas autorizaciones privadas pueden llegar a tener un gran tamaño. El tamaño de un perfil de propietario afecta al rendimiento cuando se visualiza y se trabaja con la autorización sobre objetos de propiedad y cuando se salvan o se restauran perfiles. Las operaciones del sistema también pueden resultar afectadas. Para evitar repercusiones en el rendimiento o en las operaciones del sistema, distribuya la propiedad de los objetos entre múltiples perfiles. **No asigne todos los objetos (o casi todos) a un único perfil de propietario.**

Análisis de programas que adoptan autorizaciones

Los programas que adoptan la autorización de un usuario con la autorización especial *ALLOBJ representan un riesgo para la seguridad. Puede utilizarse el siguiente método para buscar e inspeccionar esos programa:

1. Para cada usuario con la autorización especial *ALLOBJ, utilice el mandato Visualizar programas que adoptan (DSPPGMADP) para listar los programas que adoptan la autorización de ese usuario:

```
DSPPGMADP
USRPRF(nombre perfil usuario) +
          OUTPUT(*PRINT)
```

Nota: El tema “Imprimir perfiles de usuario seleccionados” en la página 55 muestra cómo listar usuarios con autorización *ALLOBJ.

2. Utilice el mandato DSPOBJAUT para determinar quién tiene autorización para utilizar cada programa que adopta y qué autorización de uso público existe para el programa:

```
DSPOBJAUT OBJ(nombre-biblioteca/nombre-programa) +
          OBJTYPE(*PGM) ASPDEV(nombre-biblioteca/nombre-programa) +
          OUTPUT(*PRINT)
```

3. Inspeccione el código fuente y la descripción de programa para evaluar lo siguiente:
   - Si se impide al usuario del programa un exceso de funciones, por ejemplo utilizar una línea de mandatos, mientras trabaja con el perfil adoptado.
   - Si el programa adopta el nivel de autorización mínimo necesario para la función deseada. Las aplicaciones que utilizan anomalía de programa pueden diseñarse utilizando el mismo perfil de propietario para los objetos y los programas. Cuando la autorización del propietario del programa es adoptada, el usuario tiene autorización total (*ALL) sobre los objetos de la aplicación. En muchos casos, el perfil de propietario no necesita ninguna autorización especial.
4. Verifique cuándo se modificó el programa por última vez, utilizando el mandato DSPOBJD:

```
DSPOBJD OBJ(nombre-biblioteca/nombre-programa) +
        OBJTYPE(*PGM) ASPDEV(nombre-biblioteca/nombre-programa) +
        DETAIL(*FULL)
```

Gestión del diario de auditoría y receptores de diario

El diario de auditoría, QSYS/QAUDJRN, está pensado solamente para la auditoría de seguridad. No deben registrarse objetos en el diario de auditoría. El control de compromiso no deberá utilizar el diario de auditoría. No deben enviarse entradas de usuario a este diario utilizando el mandato Enviar entrada de diario (SNDJRNE) o la API Enviar entrada de diario (QJOSJRNE).

Se utiliza una protección especial por bloqueo para asegurar que el sistema puede grabar entradas de auditoría en el diario de auditoría. Cuando la auditoría está activa (el valor del sistema QAUDCTL no es *NONE), el trabajo árbitro del sistema (QSYSARB) mantiene un bloqueo en el diario QSYS/QAUDJRN. No podrá realizar determinadas operaciones en el diario de auditoría mientras la auditoría esté activa, por ejemplo:

- Mandato DLTJRN
- Mandato ENDJRNxxx
- Mandato APYJRNCHG
- Mandato RMVJRNCHG
- Mandato DMPOBJ o DMPSYSOBJ
- Mover el diario
- Restaurar el diario
- Operaciones que funcionen con autorización, por ejemplo el mandato GRTOBJAUT
- Mandato WRKJRN

La información grabada en las entradas de diario de seguridad está descrita en el *Seguridad, Manual de consulta*. Todas las entradas de seguridad del diario de auditoría tienen un código de diario T. En el diario QAUDJRN, aparte de entradas de seguridad, aparecen entradas del sistema. Son entradas con un código de diario J, relacionadas con la carga del programa inicial (IPL) y operaciones generales realizadas en los receptores de diario (por ejemplo, salvar el receptor).

Si se producen daños en el diario o en su receptor actual de forma que no pueden registrarse las entradas de auditoría, el valor del sistema QAUDENDACN determina la acción que llevará a cabo el sistema. La recuperación de un diario o un receptor de diario dañados es igual que para los demás diarios.

Puede interesarle hacer que el sistema gestione el cambio de receptores de diario. Especifique MNGRCV(*SYSTEM) al crear el diario QAUDJRN, o bien modifique el diario para que tenga ese valor. Si especifica MNGRCV(*SYSTEM), el sistema desconecta automáticamente el receptor cuando llega al umbral de tamaño y crea y conecta un nuevo receptor de diario. Esto se denomina **Gestión de cambio de diario del sistema**. Consulte iSeries Information Center—>Gestión de sistemas–>Gestión de diarios–>Gestión de diario local–>Gestionar diarios, para obtener más información. Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Capítulo 6. Gestión de autorizaciones

Hay disponible un conjunto de informes de seguridad para ayudarle a hacer un seguimiento de cómo está configurada la autorización en su sistema. Al ejecutar estos informes de forma inicial, puede imprimirlo todo (autorización para todos los archivos o para todos los programas, por ejemplo).

Después de haber establecido la base de información, puede ejecutar regularmente las versiones cambiadas de informe. La versiones cambiadas ayudan a identificar cambios relevantes para la seguridad en el sistema a los que se deba prestar atención. Por ejemplo, puede ejecutar el informe que muestre la autorización de uso público para los archivos cada semana. Puede pedir sólo la versión cambiada del informe. En él se mostrarán los archivos nuevos en el sistema que están disponibles para todo el mundo y los archivos existentes cuya autorización de uso público haya cambiado desde el último informe.

Hay dos menús disponibles para ejecutar herramientas de seguridad:

- Utilice el menú SECTOOLS para ejecutar programas interactivamente.
- Utilice el menú SECBATCH para ejecutar programas por lotes. El menú SECBATCH tiene dos partes: una para someter los trabajos inmediatamente a la cola de trabajos y la otra para colocar los trabajos en el planificador de trabajos.

Si está utilizando iSeries Navigator, siga estos pasos para ejecutar las herramientas de seguridad:

1. En iSeries Navigator, expanda el Servidor—>**Seguridad**.
2. Pulse con el botón derecho del ratón en **Políticas** y seleccione **Explorar** para visualizar una lista de políticas que puede crear y gestionar.

Supervisión de la autorización de uso público sobre objetos

Por motivos de simplicidad y rendimiento, la mayoría de los sistemas están preparados de tal modo que la mayor parte de los objetos están disponibles para muchos usuarios. A los usuarios se les deniega explícitamente el acceso a ciertos objetos confidenciales en lugar de tener autorización expresa para utilizar todos los objetos. Algunos sistemas con requisitos de seguridad más restrictivos tienen el enfoque opuesto y proporcionan autorización sobre objetos explícitamente. En estos sistemas, la mayoría de los objetos se crean con la autorización de uso público *EXCLUDE.

iSeries es un sistema basado en objetos con numerosos tipos de objetos.La mayor parte de ellos no contienen información confidencial ni realizan funciones relacionadas con la seguridad. Como administrador de seguridad de un iSeries con los requisitos de seguridad habituales, tal vez desee concentrar su atención en los objetos que precisan protección, como los archivos de base de datos y los programas.Para los demás tipos de objetos, puede establecer una autorización de uso público suficiente para las aplicaciones, que es *USE para la mayor parte de tipos de objetos.

Puede utilizar el mandato Imprimir autorización de uso público (PRTPUBAUT) para imprimir información sobre los objetos a los que los usuarios públicos pueden acceder. (Un **usuario público** es aquel que tiene autorización de inicio de sesión y que no tiene autorización explícita sobre un objeto.) Al utilizar el mandato

PRTPUBAUT, puede especificar los tipos de objeto y las bibliotecas o directorios que desee examinar. En los menús SECBATCH y SECTOOLS hay opciones para imprimir el Informe de objetos con autorización de uso público de los tipos de objetos que suelen tener consideraciones de seguridad. Puede imprimir la versión modificada de este informe regularmente para ver qué objetos precisan su atención.

Gestión de autorizaciones para objetos nuevos

OS/400 proporciona funciones para ayudarle a gestionar la autorización y la propiedad de nuevos objetos del sistema. Cuando un usuario crea un objeto nuevo, el sistema determina lo siguiente:

- Quién será el propietario del objeto
- Cuál es la autorización pública para el objeto
- Si el objeto tendrá autorizaciones privadas
- Dónde colocar el objeto (qué biblioteca o directorio)
- Si se auditará el acceso al objeto

El sistema utiliza valores del sistema, parámetros de biblioteca y parámetros de perfil de usuario para tomar estas decisiones. "Assigning Authority and Ownership to New Objects " en el capítulo 5 de la publicación *iSeries Security Reference* proporciona numerosos ejemplos de las opciones disponibles.

Puede utilizar el mandato PRTUSRPRF para imprimir los parámetros de perfil de usuario que afectan a la propiedad y a la autorización para objetos nuevos. La Figura 5 en la página 67 muestra un ejemplo de este informe.

Supervisión de listas de autorizaciones

Puede agrupar los objetos con requisitos de seguridad similares utilizando una lista de autorizaciones. Conceptualmente, una lista de autorizaciones contiene una lista de los usuarios y las autorizaciones que estos tienen sobre los objetos protegidos por la lista. Las listas de autorizaciones constituyen un modo eficaz de gestionar la autorización de objetos similares del sistema. Sin embargo, en algunos casos, dificultan el seguimiento de las autorizaciones sobre los objetos.

Puede utilizar el mandato Imprimir autorización privada (PRTPVTAUT) para imprimir información acerca de las autorizaciones sobre la lista de autorizaciones. La Figura 3 muestra un ejemplo del informe.

```
Autorizaciones privadas (informe completo)
                                                                                SYSTEM4
   Lista                  Grupo                              Gest  ----------Objeto-----------  ------------Datos-----------
  autoriz.      Propiet.  primario    Usuario     Autoriz.   List. Opr  Gest Exist  Alter  Ref  Lect  Añ.  Act. Supr Ejecutar
  LIST1         QSECOFR   *NONE       *PUBLIC     *EXCLUDE
  LIST2         BUDNIKR   *NONE       BUDNIKR     *ALL        X     X    X     X      X     X    X     X    X    X      X
                                      *PUBLIC     *CHANGE           X                          X     X    X    X      X
  LIST3         QSECOFR   *NONE       *PUBLIC     *EXCLUDE
  LIST4         CJWLDR    *NONE       CJWLDR      *ALL        X     X    X     X      X     X    X     X    X    X      X
                                      GROUP1      *ALL              X    X     X      X     X    X     X    X    X      X
                                      *PUBLIC     *EXCLUDE
```

Figura 3. Informe de autorizaciones privadas para listas de autorizaciones

Este informe contiene la misma información que la pantalla Editar lista de autorizaciones (EDTAUTL). La ventaja del informe es que concentra la información acerca de todas las listas de autorizaciones. Si, por ejemplo, está realizando la

puesta a punto de un grupo nuevo de objetos, puede buscar rápidamente en el informe si hay alguna lista de autorizaciones que cumpla los requisitos para estos objetos.

Puede imprimir una versión modificada del informe para ver las listas de autorizaciones nuevas o las que han sufrido cambios en las autorizaciones desde la última vez que se imprimió el informe. También tiene la opción de imprimir una lista de los objetos protegidos por cada lista de autorizaciones. La Figura 4 muestra un ejemplo del informe correspondiente a una lista de autorizaciones:

```
                  Visualizar objetos de lista de autorizaciones
Lista de autorizaciones  . . . . . :   CUSTAUTL
  Biblioteca . . . . . . . . . . . :     QSYS
Propietario  . . . . . . . . . . . :   AROWNER
Grupo primario . . . . . . . . . . :   *NONE

                                                          Grupo
Objeto         Biblioteca     Tipo         Propietario    primario       Texto
CUSTMAS        CUSTLIB        *FILE        AROWNER        *NONE
CUSTORD        CUSTORD        *FILE        OEOWNER        *NONE
```

Figura 4. Informe Visualizar objetos de lista de autorizaciones

Puede utilizar este informe, por ejemplo, para ver el efecto de la adición de un nuevo usuario a una lista de autorizaciones (qué autorizaciones recibirá el usuario).

Utilización de listas de autorizaciones

iSeries Navigator proporciona funciones de seguridad diseñadas para ayudarle a desarrollar un plan y una política de seguridad y para configurar el sistema para ajustarse a las necesidades de su empresa. Una de las funciones disponibles es el uso de listas de autorizaciones.

Las listas de autorizaciones tienen las siguientes características.

- Una lista de autorizaciones agrupa los objetos con requisitos de seguridad similares.
- Una lista de autorizaciones contiene conceptualmente una lista de usuarios y grupos y la autorización que cada uno tiene sobre los objetos protegidos por la lista.
- Cada usuario y grupo puede tener una autorización distinta sobre el conjunto de objetos que la lista protege.
- La autorización puede entregarse mediante la lista, en lugar de a grupos y usuarios individuales.

Las tareas que pueden realizarse utilizando listas de autorizaciones incluyen las siguientes.

- Crear una lista de autorizaciones
- Modificar una lista de autorizaciones.
- Añadir usuarios y grupos.
- Modificar permisos de usuarios.
- Visualizar objetos protegidos.

Para utilizar esta función, lleve a cabo los pasos siguientes:

1. En iSeries Navigator, expanda el servidor—>Seguridad. Verá **Listas de autorizaciones** y **Políticas**.

2. Pulse con el botón derecho del ratón en **Listas de autorizaciones** y seleccione **Lista de autorizaciones nueva**. La **Lista de autorizaciones nueva** le permite hacer lo siguiente.
   - **Uso:** Permite el acceso a los atributos del objeto y el uso del objeto. El público puede ver los objetos pero no puede modificarlos.
   - **Cambio:** Permite cambiar el contenido del objeto (con algunas excepciones).
   - **Total:** Permite todas las operaciones sobre el objeto, excepto las limitadas al propietario. El usuario o grupo puede controlar la existencia del objeto, especificar la seguridad para el objeto, modificar el objeto y realizar funciones básicas sobre el objeto. El usuario o grupo también puede cambiar la propiedad del objeto.
   - **Exclusión:** Se prohíben todas las operaciones sobre el objeto. No se permite el acceso al objeto ni operaciones sobre el mismo para los usuarios y grupos que tengan este permiso. Especifica que no se permite al público el uso del objeto.

Al trabajar con listas de autorizaciones le interesa otorgar permisos tanto para los objetos como para los datos. Los permisos sobre objetos que puede elegir se enumeran a continuación.
- **Operativo:** Proporciona el permiso para ver la descripción de un objeto y utilizar el objeto tal como determina el permiso de datos que el usuario o grupo tiene sobre ese objeto.
- **Gestión:** Proporciona el permiso para especificar la seguridad para el objeto, mover o redenominar el objeto y añadir miembros a los archivos de base de datos.
- **Existencia:** Proporciona el permiso para controlar la existencia y la propiedad del objeto. El usuario o grupo puede suprimir el objeto, liberar almacenamiento del objeto, efectuar operaciones de salvar y restaurar para el objeto y transferir la propiedad del objeto. Si un usuario o un grupo tiene un permiso de salvar especial, el usuario o grupo no necesitará el permiso de existencia para el objeto.
- **Alteración** (utilizado solamente para archivos de base de datos y paquetes SQL): Proporciona el permiso necesario para alterar los atributos de un objeto. Si el usuario o grupo tiene este permiso sobre un archivo de base de datos, el usuario o grupo puede añadir o eliminar desencadenantes, añadir o eliminar restricciones referenciales y de unicidad, así como modificar los atributos del archivo de base de datos. Si el usuario o grupo tiene este permiso sobre un paquete SQL, el usuario o grupo puede modificar los atributos del paquete SQL. Actualmente, este permiso se utiliza solamente para archivos de base de datos y paquetes SQL.
- **Referencia** (utilizado solamente para archivos de base de datos y paquetes SQL): Proporciona el permiso necesario para referenciar un objeto desde otro objeto, de forma que las operaciones sobre ese objeto puedan ser restringidas por el otro objeto. Si el usuario o grupo tiene este permiso sobre un archivo físico, el usuario o grupo puede añadir restricciones referenciales en las que el archivo físico sea el padre. Actualmente, este permiso se utiliza solamente para los archivos de base de datos.

Los permisos sobre datos que puede elegir se enumeran a continuación.
- **Lectura:** Proporciona el permiso necesario para obtener y visualizar el contenido del objeto, por ejemplo ver registros de un archivo.
- **Adición:** Proporciona el permiso para añadir entradas a un objeto, por ejemplo añadir mensajes a una cola de mensajes o añadir registros a un archivo.
- **Actualización:** Proporciona el permiso para cambiar las entradas de un objeto, por ejemplo cambiar registros de un archivo.

- **Supresión:** Proporciona el permiso para eliminar entradas de un objeto, por ejemplo eliminar mensajes de una cola de mensajes o suprimir registros de un archivo.
- **Ejecución:** Proporciona el permiso necesario para ejecutar un programa, un programa de servicio o un paquete SQL. El usuario también puede ubicar un objeto en una biblioteca o directorio.

Para obtener más información sobre cada proceso a medida que cree o edite sus listas de autorizaciones, utilice la ayuda en línea disponible en iSeries Navigator.

Acceso a políticas en iSeries Navigator

Puede utilizar iSeries Navigator para ver y gestionar políticas para su servidor iSeries. iSeries Navigator tiene cinco áreas de políticas:

- **Política de auditorías**
  Le permite configurar la supervisión de acciones específicas y acceder a recursos específicos de su sistema.
- **Política de seguridad**
  Le permite especificar el nivel de seguridad y opciones adicionales relacionadas con la seguridad del sistema.
- **Política de contraseñas**
  Le permite especificar el nivel de contraseña para el sistema.
- **Política de restauración**
  Le permite especificar cómo se restauran determinados objetos en el sistema.
- **Política de inicio de sesión**
  Le permite especificar cómo los usuarios pueden iniciar la sesión en el sistema.

Para ver o modificar políticas con iSeries Navigator, siga estos pasos:

1. En iSeries Navigator, expanda su servidor—>**Seguridad**.
2. Pulse con el botón derecho del ratón en **Políticas** y seleccione **Explorar** para visualizar una lista de políticas que puede crear y gestionar. Consulte la ayuda de iSeries Navigator para obtener detalles específicos sobre estas políticas.

Supervisión de la autorización privada sobre objetos

Opciones del menú SECBATCH:
12 *para someter inmediatamente* **41** *para utilizar el planificador de trabajos*

Puede utilizar el mandato Imprimir autorización privada (PRTPVTAUT) para imprimir una lista de todas las autorizaciones privadas correspondientes a los objetos de un tipo determinado de una biblioteca especificada.

Puede utilizar este informe para detectar las nuevas autorizaciones sobre objetos. También puede serle útil para evitar que la estructura de autorizaciones privadas se convierta en complicada e imposible de gestionar.

Supervisión del acceso a colas de salida y de trabajos

En algunos casos, los administradores de seguridad hacen un gran trabajo a fin de proteger el acceso a los archivos, pero se olvidan de lo que sucede cuando el contenido de un archivo se imprime. Los servidores iSeries proporcionan funciones para proteger las colas de salida y las colas de trabajos confidenciales. Puede

proteger una cola de salida para que los usuarios no autorizados no puedan, por ejemplo, ver o copiar los archivos en spool confidenciales que están a la espera de imprimirse. También puede proteger las colas de trabajos para que los usuarios no autorizados no puedan redirigir un trabajo confidencial a una cola de salida no confidencial ni cancelar el trabajo.

Opciones del menú SECBATCH:
24 para someter inmediatamente 63 *para utilizar el planificador de trabajos*

El tema *Seguridad básica del sistema y planificación* del Information Center y las publicaciones *iSeries Security Reference*, describen cómo proteger las colas de salida y las colas de trabajos.

Puede utilizar el mandato Imprimir autorización sobre cola (PRTQAUT) para imprimir los valores de seguridad correspondientes a las colas de trabajos y de salida del sistema. A continuación puede evaluar la impresión de trabajos que contienen información confidencial y asegurarse de que van a parar a colas de salida y de trabajos que están protegidas.

Para las colas de salida y de trabajos que considera susceptibles de seguridad, puede comparar los valores de seguridad con la información del Apéndice D de la publicación *iSeries Security Reference*. Las tablas del Apéndice D indican qué valores son necesarios para realizar distintas funciones de cola de salida y de trabajos.

Supervisión de autorizaciones especiales

Si los usuarios del sistema tienen autorizaciones especiales innecesarias, sus esfuerzos para desarrollar un esquema de autorización sobre objeto adecuado pueden ser inútiles. La autorización sobre objeto no tiene ningún significado si un perfil de usuario tiene la autorización especial *ALLOBJ. Un usuario que tenga la autorización especial *SPLCTL puede ver todos los archivos en spool del sistema, independientemente de los esfuerzos que realice para proteger las colas de salida. Los usuarios con la autorización especial *JOBCTL, pueden afectar las operaciones del sistema y redirigir los trabajos. Los usuarios con la autorización especial *SERVICE pueden utilizar las herramientas de servicio para acceder a los datos sin pasar por el sistema operativo.

Opciones del menú SECBATCH:
29 para someter inmediatamente 68 *para utilizar el planificador de trabajos*

Puede utilizar el mandato Imprimir perfil de usuario (PRTUSRPRF) para imprimir información acerca de las autorizaciones especiales y las clases de usuario correspondientes a los perfiles de usuario del sistema. Cuando se ejecuta el informe, se dispone de varias opciones:
- Todos los perfiles de usuario
- Perfiles de usuario con autorizaciones especiales específicas
- Perfiles de usuario que tengan clases de usuario específicas
- Perfiles de usuario con discrepancias entre la clase de usuario y las autorizaciones especiales.

La Figura 5 muestra un ejemplo del informe que contiene las autorizaciones especiales para todos los perfiles de usuario:

```
                                    Información de perfil de usuario
Tipo de informe  . . . . . :   *AUTINFO
Seleccionar por  . . . . . :   *SPCAUT
Autorizaciones especiales  . . :   *ALL
                          -----------Autorizaciones especiales---------
                                    *IO                                                                 Tipo
Perfil    Perfiles  *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Clase                Propiet   Autoriz.   autoriz.   Posibilidad
usuario   grupo      OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  usuario    Propiet   grupo      grupo      limitada
USERA     *NONE      X     X    X     X     X     X     X     X    *SECOFR    *USRPRF   *NONE      *PRIVATE   *NO
USERB     *NONE                      X     X                       *PGMR      *USRPRF   *NONE      *PRIVATE   *NO
USERC     *NONE      X     X    X     X     X     X     X     X    *SECOFR    *USRPRF   *NONE      *PRIVATE   *NO
USERD     *NONE                                                    *USER      *USRPRF   *NONE      *PRIVATE   *NO
```

Figura 5. Informe de Información de usuario: Ejemplo 1

Además de las autorizaciones especiales, el informe contiene lo siguiente:

- Si el perfil de usuario tiene posibilidades limitadas.
- Si el usuario o el grupo de usuarios es propietario de los objetos nuevos que cree el usuario.
- Qué autorización recibirá automáticamente el grupo de usuarios sobre los nuevos objetos creados por el usuario.

La Figura 6 muestra un ejemplo del informe correspondiente a las autorizaciones especiales y clases de usuario con discrepancias:

```
Información de perfil de usuario
 Tipo de informe  . . . . . :   *AUTINFO
 Seleccionar por  . . . . . :   *MISMATCH
            ------------------------------Autorizaciones especiales---------
                                    *IO                                                                 Tipo
 Perfil    Perfiles  *ALL  *AUD  SYS  *JOB  *SAV  *SEC  *SER  *SPL  Clase                Propiet   Autoriz.   autoriz.   Posibilidad
 usuario   grupo      OBJ   IT   CFG   CTL   SYS   ADM  VICE   CTL  usuario    Propiet   grupo      grupo      limitada
 USERX     *NONE      X                 X     X                 X    *SYSOPR    *USRPRF   *NONE      *PRIVATE   *NO
 USERY     *NONE                                    X                 *USER      *USRPRF   *NONE      *PRIVATE   *NO
 USERZ                                              X                 *USER      *USRPRF   *NONE      *PRIVATE   *NO
         QPGMR                       X     X
```

Figura 6. Informe de Información de usuario: Ejemplo 2

En la Figura 6, observe lo siguiente:

- USERX tiene una clase de usuario de operador del sistema (*SYSOPR), pero tiene las autorizaciones especiales *ALLOBJ y *SPLCTL.
- USERY tiene una clase de usuario (*USER), pero tiene la autorización especial *SECADM.
- USERZ también tiene una clase de usuario (*USER), pero tiene la autorización especial *SECADM. También puede ver que USERZ es un miembro del grupo QPGMR, que tiene las autorizaciones especiales *JOBCTL y *SAVSYS.

Puede ejecutar estos informes regularmente para supervisar la administración de perfiles de usuario.

Supervisión de entornos de usuario

Una de las funciones del perfil de usuario es la definición del entorno del usuario, que comprende la cola de salida, el menú inicial y la descripción del trabajo. El entorno del usuario tiene efectos sobre el modo en que el usuario ve el sistema y, hasta cierto punto, sobre las acciones que el usuario puede realizar. El usuario debe tener autorización sobre los objetos que están especificados en el perfil de usuario.

Sin embargo, si su esquema de seguridad aún está en curso o no es muy restrictivo, el entorno de usuario definido en un perfil de usuario puede producir resultados no deseados. A continuación encontrará varios ejemplos:

Opciones del menú SECBATCH:

29 *para someter inmediatamente* **68** *para utilizar el planificador de trabajos*

- La descripción de trabajo de usuario puede especificar un perfil de usuario con más autorización que el usuario.
- El usuario puede tener un menú inicial sin línea de mandatos. Sin embargo, el programa de manejo de la tecla de atención del usuario puede proporcionar una.
- El usuario puede tener autorización para ejecutar informes confidenciales. Sin embargo, la salida del usuario puede dirigirse a una cola de salida que esté disponible para los usuarios que no deberían ver los informes.

Puede utilizar la opción *ENVINFO del mandato Imprimir perfil de usuario (PRTUSRPRF) para supervisar los entornos que están definidos para los usuarios del sistema. La Figura 7 muestra un ejemplo del informe:

```
                                    Información de perfil de usuario
Tipo de informe  . . . . . :   *ENVINFO
Seleccionar por  . . . . . :   *USRCLS
                          Menú          Programa      Descripción     Cola          Cola          Programa
Perfil         Biblioteca inicial/      inicial/        trabajo/      mensajes/     salida/       atención/
usuario        actual     biblioteca    biblioteca     biblioteca     biblioteca    biblioteca    bibliot.
AUDSECOFR      AUDITOR    MAIN          *NONE           QDFTJOBD      QSYSOPR       *WRKSTN       *SYSVAL
                          *LIBL                         QGPL          QSYS
USERA          *CRTDFT    OEMENU        *NONE           QDFTJOBD      USERA         *WRKSTN       *SYSVAL
                          *LIBL                         QGPL          QUSRSYS
USERB          *CRTDFT    INVMENU       *NONE           QDFTJOBD      USERB         *WRKSTN       *SYSVAL
                          *LIBL                         QGPL          QUSRSYS
USERC          *CRTDFT    PAYROLL       *NONE           QDFTJOBD      USERC         PAYROLL       *SYSVAL
                          *LIBL                         QGPL          QUSRSYS       PRPGMLIB
```

Figura 7. Ejemplo de imprimir perfil de usuario-entorno de usuario

Gestión de herramientas de servicio

Las herramientas de servicio se utilizan para configurar, gestionar y dar servicio a su servidor. Puede accederse a las herramientas de servicio desde las herramientas de servicio dedicado (DST) o desde las herramientas de servicio del sistema (SST). Son necesarios ID de usuario de herramientas de servicio para acceder a DST, SST y para utilizar funciones de iSeries Navigator para la gestión de particiones lógicas (LPAR) y la gestión de unidades de discos.

Las DST están disponibles cuando se ha iniciado el Código interno bajo licencia, incluso si no se ha cargado el OS/400. Las SST están disponibles en OS/400. La tabla siguiente describe las diferencias básicas entre DST y SST.

Característica	DST	SST

Cómo acceder	Acceso físico a través de la consola durante una IPL manual o seleccionando la opción 21 en el panel de control.	Acceso a través de un trabajo interactivo con la capacidad de iniciar la sesión con QSRV o las siguientes autorizaciones: • Autorización para el mandato CL STRSST (Iniciar SST). • Autorización especial de servicio (*SERVICE) o autorización especial sobre todos los objetos (*ALLOBJ). • Privilegio funcional para utilizar SST.
Cuándo está disponible	Disponible incluso cuando el servidor tiene posibilidades limitadas. No es necesario OS/400 para acceder a las DST.	Disponible cuando se ha iniciado OS/400. Es necesario OS/400 para acceder a las SST.
Cómo autenticar	Requiere un ID de usuario y una contraseña de herramientas de servicio.	Requiere un ID de usuario y una contraseña de herramientas de servicio.

Consulte iSeries Information Center—>Seguridad—>Herramientas de servicio, para obtener información sobre la utilización de las Herramientas de servicio para realizar las siguientes tareas:

- Acceder a herramientas de servicio con DST
- Acceder a herramientas de servicio con SST
- Acceder a herramientas de servicio con iSeries Navigator
- Crear un ID de usuario de herramientas de servicio
- Cambiar los privilegios funcionales de un ID de usuario de herramientas de servicio
- Cambiar la descripción de un ID de usuario de herramientas de servicio
- Visualizar un ID de usuario de herramientas de servicio
- Habilitar o inhabilitar un ID de usuario de herramientas de servicio
- Suprimir un ID de usuario de herramientas de servicio
- Cambiar los ID de usuario y las contraseñas de herramientas de servicio utilizando SST o DST
- Cambiar su ID de usuario y contraseña de herramientas de servicio utilizando STRSST
- Cambiar los ID de usuario y contraseñas de herramientas de servicio utilizando
- API Cambiar ID de usuario de herramientas de servicio (QSYCHGDS)
- Restablecer la contraseña del perfil de usuario QSECOFR de OS/400
- Restablecer el ID de usuario y la contraseña de herramientas de servicio de QSECOFR
- Salvar datos de seguridad de herramientas de servicio. Restaurar datos de seguridad de herramientas de servicio
- Crear su propia versión del ID de usuario de herramientas de servicio de QSECOFR
- Configurar el servidor de herramientas de servicio para DST
- Configurar el servidor de herramientas de servicio para OS/400
- Supervisar el uso de funciones de servicio mediante DST

- Supervisar el uso de herramientas de servicio mediante anotaciones de auditoría de seguridad de OS/400

Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Capítulo 7. Utilización de seguridad en particiones lógicas (LPAR)

Tener múltiples particiones lógicas en un solo servidor iSeries podría ser beneficioso en los siguientes casos.

- **Mantenimiento de sistemas independientes**: Dedicando una parte de los recursos (unidad de almacenamiento de disco, procesadores, memoria y dispositivos de E/S) a una partición se consigue un aislamiento lógico del software. Las particiones lógicas también tienen una cierta tolerancia a las anomalías de hardware, si se configuran correctamente. Las cargas de trabajos interactivos y de proceso por lotes, que juntas en una sola máquina es posible que no se procesasen correctamente, pueden aislarse y ejecutarse con eficacia en particiones separadas.
- **Consolidación** : Un sistema con particiones lógicas puede reducir el número de servidores iSeries necesarios dentro de una empresa. Puede consolidar varios sistemas en un único sistema con particiones lógicas. Esto elimina la necesidad de equipos adicionales y los gastos que conllevan. Puede desplazar los recursos de una partición lógica a otra a medida que cambien sus necesidades.
- **Creación de un entorno mixto de producción y prueba:** Puede crear un entorno que combine la producción y las pruebas. Puede crear una única partición de producción en la partición primaria. Para múltiples particiones de producción, vea *Creación de un entorno de múltiples particiones de producción* más abajo.

  Una partición lógica puede ser una partición de prueba o de producción. Una partición de producción ejecuta las principales aplicaciones comerciales. Una anomalía en una partición de producción podría alterar las operaciones comerciales de forma significativa y costarle tiempo y dinero. Una partición de prueba realiza pruebas en el software. Una anomalía en una partición de prueba, aunque no está planificado necesariamente, no interrumpirá las operaciones comerciales normales.
- **Creación de un entorno de múltiples particiones de producción:** Debe crear múltiples particiones de producción solamente en las particiones secundarias. En esta situación dedicará la partición primaria a la gestión de particiones.
- **Copia de seguridad en activo:** Cuando una partición secundaria se duplica en otra partición lógica dentro del mismo sistema, conmutar a la copia de seguridad durante la anomalía de la partición no provocaría grandes molestias. Esta configuración también minimiza el efecto de los períodos de salvar prolongados. Puede tener la partición de copia de seguridad fuera de línea y salvar mientras la otra partición lógica continúa realizando trabajos de producción. Necesitará software especial para utilizar esta estrategia de copia de seguridad urgente.
- **Cluster integrado:** Utilizando OptiConnect/400 y un software de aplicaciones de alta disponibilidad, el sistema con particiones puede ejecutarse como un cluster integrado. Puede utilizar un cluster integrado para proteger su sistema de la mayoría de anomalías no planificadas dentro de una partición secundaria.

Nota: Al configurar una partición secundaria es necesario realizar consideraciones adicionales para las ubicaciones de tarjetas. Si el procesador de entrada/salida (IOP) que seleccione para la consola también tiene una tarjeta de LAN y dicha tarjeta LAN no está pensada para que se utilice con la Consola de operaciones, se activará para que la utilice la consola y usted no

podrá utilizarla para sus fines. Para obtener más información sobre cómo trabajar con la Consola de operaciones, consulte Capítulo 8, “iSeries Consola de operaciones”, en la página 75.

Consulte ″Particiones lógicas″ en el iSeries Information Center para obtener información detallada sobre este tema.

Gestión de la seguridad para las particiones lógicas

Las tareas relacionadas con la seguridad que realice en un sistema con particiones serán las mismas que en un sistema sin particiones lógicas. No obstante, al crear particiones lógicas, trabaja con más de un sistema independiente. Por consiguiente, tendrá que realizar las mismas tareas en cada partición lógica en lugar de realizarlas una sola vez en un sistema sin particiones lógicas.

Estas son algunas de las normas básicas a recordar al tratar la seguridad en las particiones lógicas:

- Se añaden los usuarios a las particiones lógicas del sistema de una partición en una. Es necesario añadir los usuarios a cada partición lógica a la que desee que accedan.
- Limite el número de personas que tengan autorización para ir a las herramientas de servicio dedicado (DST) y a las herramientas de servicio del sistema (SST) en la partición primaria. Consulte el tema ″Gestión de particiones lógicas mediante iSeries Navigator, DST y SST″ en el iSeries Information Center para obtener más informacióm sobre DST y SST. Consulte “Gestión de herramientas de servicio” en la página 68 para obtener información sobre el uso de perfiles de usuario de herramientas de servicio para controlar el acceso a las actividades de las particiones.

  Nota: Debe inicializar el Service Tools Server (STS) antes de utilizar iSeries Navigator para acceder a las funciones LPAR. Consulte iSeries Information Center—>Seguridad—>Herramientas de servicio para obtener información relacionada. Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.
- Las particiones secundarias no pueden ver ni utilizar el almacenamiento principal y las unidades de discos de otra partición lógica.
- Las particiones secundarias solamente pueden ver sus propios recursos de hardware.
- La partición primaria puede ver todos los recursos de hardware del sistema en las pantallas Trabajar con particiones del sistema de DST y SST.
- El sistema operativo de la partición primaria sigue viendo solamente sus recursos disponibles.
- El panel de control del sistema controla la partición primaria. Cuando establece la modalidad del panel en Protegido (Secure), no pueden llevarse a cabo acciones en la pantalla Trabajar con estado de las particiones desde SST. Para forzar DST desde el panel de control del sistema, debe cambiar la modalidad a Manual.
- Cuando establece la modalidad de operación de una partición secundaria como protegida, restringe el uso de Trabajar con estado de las particiones de las siguientes maneras:
  - Solamente puede utilizar DST en la partición secundaria para cambiar el estado de la partición; no puede utilizar SST para cambiar el estado de particiones.

- Solamente puede forzar DST en la partición secundaria desde la pantalla Trabajar con estado de las particiones de la partición primaria utilizando DST o SST.
- Solamente puede utilizar DST en la partición primaria para cambiar la modalidad de una partición secundaria de protegida a cualquier otro valor.

Una vez la modalidad de una partición secundaria ya no es la de protegida, puede utilizar DST y SST en la partición secundaria para cambiar el estado de la partición.

Para obtener más información sobre la seguridad en el servidoriSeries, consulte el Manual de consulta de seguridad y las páginas sobre Seguridad básica del sistema y planificación de iSeries Information Center.

Capítulo 8. iSeries Consola de operaciones

La Consola de operaciones le permite utilizar el PC para el acceso y el control del servidor iSeries. La Consola de operaciones incluye soporte para la marcación de PC remoto a servidores iSeries sin dispositivos de consola, permitiendo a los PC remotos convertirse en las consolas. Cuando utilice la Consola de operaciones, tenga en cuenta lo siguiente:

- Desde la Consola de operaciones puede llevar a cabo las mismas tareas que realizaba desde una consola tradicional. Por ejemplo, los perfiles de usuario que tienen autorización especial *SERVICE o *ALLOBJ pueden iniciar la sesión en la Consola de operaciones, incluso si están inhabilitados.
- La Consola de operaciones utiliza perfiles de usuario y contraseñas de herramientas de servicio para habilitar la conexión con el servidor iSeries. Esto hace que sea de especial importancia modificar sus perfiles de usuario y contraseñas de herramientas de servicio. Es posible que los intrusos estén familiarizados con los ID de usuario y las contraseñas por omisión de los perfiles de usuario de herramientas de servicio, por lo que podrían utilizarlos para intentar establecer una sesión de consola remota en el servidor iSeries. Vea "Cambio de contraseñas conocidas" en la página 21 y "Evitar contraseñas por omisión" en la página 27 para obtener consejos sobre las contraseñas.
- Para proteger su información al utilizar la Consola remota, utilice la opción de retorno de llamada de las Redes de marcación Windows.
- Al configurar una partición secundaria es necesario realizar consideraciones adicionales para las ubicaciones de tarjetas. Si el procesador de entrada/salida (IOP) que seleccione para la consola también tiene una tarjeta de LAN y dicha tarjeta LAN no está pensada para que se utilice con la Consola de operaciones, la consola la activará y puede que usted no pueda utilizarla.

En la V5R1, se ha mejorado la Consola de operaciones para permitir que se realicen actividades de consola en una red de área local (LAN). La mejora en la autenticación y el cifrado de datos proporciona seguridad de red para los procedimientos de consola. Para utilizar la Consola de operaciones con conectividad LAN, se recomienda encarecidamente que instale los siguientes productos:

- Cryptographic Access Provider, 5722–AC2 ó 5722–AC3 en el servidor iSeries
- Client Encryption, 5722–CE2 ó 5722–CE3 en el PC Consola de operaciones

Para que se cifren los datos de la consola, el servidor iSeries debe tener instalado uno de los productos Cryptographic Access Provider **y** el PC debe tener instalado uno de los productos Client Encryption.

Nota: Si no se instala ningún producto criptográfico no habrá cifrado de datos.

La tabla siguiente resume los resultados de cifrado de los productos disponibles:

Tabla 13. Resultados de cifrado

Cryptographic Access Provider en el servidor iSeries	Client Encryption en el PC Consola de operaciones	Cifrado de datos resultante
NONE	NONE	NONE
5722–AC2	5722–CE2	56 bits

Tabla 13. Resultados de cifrado (continuación)

Cryptographic Access Provider en el servidor iSeries	Client Encryption en el PC Consola de operaciones	Cifrado de datos resultante
5722–AC2	5722–CE3	56 bits
5722–AC3	5722–CE2	56 bits
5722–AC3	5722–CE3	128 bits

Para obtener información adicional sobre la puesta a punto y la administración de iSeries Consola de operaciones, consulte iSeries Information Center.

Visión general de la seguridad de la Consola de operaciones

La seguridad de la Consola de operaciones consta de:

- autenticación del dispositivo de consola
- autenticación de usuario
- privacidad de los datos
- integridad de los datos

La Consola de operaciones con conectividad directa tiene implícitas la autenticación de dispositivo, la privacidad de datos y la integridad de datos debido a su conexión punto a punto. La seguridad de autenticación de usuario es necesaria para iniciar la sesión en la pantalla de la consola.

Autenticación de dispositivos de consola

La autenticación del dispositivo de consola asegura qué dispositivo físico es la consola. La Consola de operaciones con conectividad directa utiliza una conexión física similar a una consola twinaxial. La Consola de operaciones que utiliza una conexión directa puede protegerse físicamente de forma similar a una conexión twinaxial para controlar el acceso al dispositivo de consola físico.

La Consola de operaciones con conectividad LAN utiliza una versión de la capa de sockets segura (SSL) que soporta la autenticación de dispositivos y usuarios pero sin utilizar certificados. Para esta forma de conexión, la autenticación de dispositivo se basa en un perfil de dispositivo de herramientas de servicio. Consulte la página 77 para obtener más detalles.

Autenticación de usuario

La autenticación de usuario proporciona una garantía sobre quién está utilizando el dispositivo de consola. Todos los temas relacionados con la autenticación de usuario son los mismos, independientemente del tipo de consola.

Privacidad de datos

La privacidad de datos proporciona la seguridad de que los datos de la consola solamente podrá leerlos el destinatario correcto. La Consola de operaciones con conectividad directa utiliza una conexión física similar a una consola twinaxial o una conexión de red segura para que la conectividad de la LAN proteja los datos de la consola. La Consola de operaciones que utiliza una conexión directa tiene la misma privacidad de datos que una conexión twinaxial. Si la conexión física es segura, los datos de la consola permanecen protegidos.

La Consola de operaciones con conectividad LAN utiliza una conexión de red segura si están instalados los productos criptográficos adecuados (ACx y CEx). La sesión de consola utiliza el cifrado más potente posible dependiendo de los productos criptográficos instalados en el servidor iSeries y en el PC que ejecute la Consola de operaciones.

Nota: Si no se instala ningún producto criptográfico, no habrá cifrado de datos.

Integridad de datos

La integridad de datos proporciona la seguridad de que los datos de la consola no han cambiado por el camino hasta el destinatario. La Consola de operaciones con conectividad directa utiliza una conexión física similar a una consola twinaxial o una conexión de red segura para que la conectividad de la LAN proteja los datos de la consola. La Consola de operaciones que utiliza una conexión directa tiene la misma integridad de datos que una conexión twinaxial. Si la conexión física es segura, los datos de la consola permanecen protegidos.

La Consola de operaciones con conectividad LAN utiliza una conexión de red segura si están instalados los productos criptográficos adecuados (ACx y CEx). La sesión de consola utiliza el cifrado más potente posible dependiendo de los productos criptográficos instalados en el servidor iSeries y en el PC que ejecute la Consola de operaciones.

Nota: Si no se instala ningún producto criptográfico, no habrá cifrado de datos.

Utilización de la Consola de operaciones con conectividad LAN

Nota: Cualquier dispositivo de Consola de operaciones puede ser una consola, pero solamente las configuraciones con base LAN utilizan el perfil de usuario de herramientas de servicio.

El servidor iSeries se entrega con un perfil de dispositivo de herramientas de servicio por omisión QCONSOLE, con una contraseña por omisión QCONSOLE. La Consola de operaciones con conectividad LAN cambiará la contraseña durante cada conexión satisfactoria. Vea “Utilización del asistente de configuración de la Consola de operaciones” en la página 78 para obtener más información.

Para obtener información adicional sobre iSeries Consola de operaciones con conectividad LAN, consulte el tema Configurar la Consola de operaciones con conectividad LAN, en Information Center.

Protección de la Consola de operaciones con conectividad LAN

Al utilizar la Consola de operaciones con conectividad LAN, se recomienda llevar a cabo las siguientes acciones:

- Cree otro perfil de dispositivo de herramientas de servicio con atributos de consola y guarde la información del perfil en un lugar seguro.
- Instale Cryptographic Access Provider, 5722–AC2 ó 5722–AC3 en el servidor iSeries y Client Encryption, 5722–CE2 ó 5722–CE3 en el PC Consola de operaciones.
- Elija una contraseña de información de dispositivo de servicio que no sea trivial.
- Proteja el PC Consola de operaciones de la misma manera que protegería una consola twinaxial o una Consola de operaciones con conectividad directa.

Utilización del asistente de configuración de la Consola de operaciones

El asistente de configuración añadirá la información necesaria al PC al utilizar la Consola de operaciones con conectividad LAN. El asistente de configuración solicita el perfil de dispositivo de herramientas de servicio, la contraseña de perfil de dispositivo de herramientas de servicio y una contraseña para proteger la información del perfil de dispositivo de herramientas de servicio.

Nota: La contraseña de la información del perfil de dispositivo de herramientas de servicio se utiliza para bloquear y desbloquear la información del perfil de dispositivo de herramientas de servicio (perfil de dispositivo de herramientas de servicio y contraseña) en el PC.

Al establecer una conexión de red, el asistente de configuración de la Consola de operaciones le solicitará la contraseña de la información de dispositivo de servicio para acceder al perfil de dispositivo de herramientas de servicio y contraseña que están cifrados. También se le solicitará una identificación de usuario y contraseña de herramientas de servicio válidos.

Capítulo 9. Detección de programas sospechosos

Las últimas tendencias en la utilización de sistemas informáticos han aumentado la probabilidad de que el sistema tenga programas de fuentes no fiables o programas que llevan a cabo funciones desconocidas. Ejemplos de esto son:

- Un usuario de PC a menudo obtiene programas de otros usuarios de PC. Si el PC está conectado al sistema iSeries, el programa puede afectar al servidor iSeries.
- Los usuarios que se conectan a redes también pueden obtener programas, por ejemplo, de los tablones de anuncios.
- Los piratas informáticos se han vuelto cada vez más activos y famosos. A menudo publican sus métodos y sus resultados. Esto puede llevar a su imitación por parte de programadores que son normalmente respetuosos con la ley.

Estas tendencias han conducido a un problema en la seguridad de los sistemas que se denomina **virus informático**. Un virus es un programa que puede modificar otros programas para incluir una copia de sí mismo. Los demás programas quedan entonces infectados por el virus. Además, el virus puede realizar otras operaciones que pueden ocupar recursos del sistema o destruir datos.

La arquitectura del servidor iSeries proporciona cierta protección contra las características infecciosas de un virus informático. Esto se describe en el apartado "Protección contra los virus informáticos". Un administrador de seguridad de un servidor iSeries debe preocuparse más de los programas que realizan funciones no autorizadas. Los temas restantes de este capítulo describen las maneras en que alguien con intenciones poco fiables puede preparar programas dañinos para ejecutarlos en el sistema. Los temas proporcionan consejos para evitar que los programas lleven a cabo funciones no autorizadas.

Consejo de seguridad

La autorización sobre objetos es siempre la primera línea de defensa. Si no tiene un buen plan para proteger los objetos, el sistema estará indefenso. En este apartado se tratan las maneras en que un usuario autorizado puede intentar sacar partido de los agujeros del esquema de autorización de objetos.

Protección contra los virus informáticos

Un sistema que tiene una infección por virus tiene un programa que puede cambiar otros programas. La arquitectura del iSeries, basada en objetos, hace más difícil que alguien produzca y disperse este tipo de virus en esta arquitectura que en otras arquitecturas de sistemas. En el servidor iSeries, puede utilizar mandatos específicos e instrucciones para trabajar en cada tipo de objeto. No puede utilizar una instrucción de archivo para cambiar un objeto de programa operativo (que es lo que hacen la mayoría de los creadores de virus). Tampoco puede crear fácilmente un programa que cambie otro objeto de programa. Para hacer esto es necesario un tiempo, un esfuerzo y una habilidad considerables y también es necesario tener acceso a herramientas y documentación que no están disponibles generalmente.

Sin embargo, debido a que hay funciones nuevas del servidor iSeries que están disponibles para participar en el entorno de sistemas abiertos, algunas de las funciones de protección basadas en objetos de los servidores iSeries ya no son aplicables. Por ejemplo, con el sistema de archivos integrado (IFS), los usuarios pueden manipular directamente algunos objetos en los directorios, tales como archivos continuos.

Además, a pesar de que la arquitectura del servidor iSeries dificulta que un virus se disperse entre programas del servidor iSeries, su arquitectura no evita que un servidor iSeries sea un portador de un virus. Como servidor de archivos, el servidor iSeries puede almacenar programas que comparten muchos usuarios de PC. Alguno de estos programas puede contener un virus que el servidor iSeries no detecte. Para evitar que este tipo de virus infecte los PC conectados al servidor del iSeries, debe utilizar software de detección de virus para PC.

Existen varias funciones en el servidor iSeries para evitar que alguien utilice un lenguaje de bajo nivel con soporte para punteros para alterar un programa objeto operativo:

- Si el sistema funciona a un nivel de seguridad 40 o superior, la protección de integridad incluye protecciones contra el cambio de los objetos de programa. Por ejemplo, no se puede ejecutar satisfactoriamente un programa que contiene instrucciones de máquina bloqueadas (protegidas).
- El valor de validación del programa también está pensado como protección al restaurar un programa salvado (y potencialmente cambiado) en otro sistema. En el capítulo 2 de la publicación *iSeries Security Reference* se describen las funciones de protección de la seguridad para el nivel de seguridad 40 y superior, incluyendo valores de validación del programa.

  Nota: El valor de validación del programa no es infalible y no sustituye a la vigilancia de la evaluación de los programas que se restauran en el sistema.

Algunas herramientas también están disponibles para ayudarle a detectar la introducción de un programa alterado en el sistema:

- Puede utilizar el mandato Comprobar integridad de objetos (CHKOBJITG) para explorar los objetos (objetos operables) que cumplan los valores de búsqueda, para asegurarse de que esos objetos no fueron alterados. Esto es parecido a una función de detección de virus.
- Puede utilizar la función de auditoría de seguridad para supervisar los programas cambiados o restaurados. Los valores *PGMFAIL, *SAVRST y *SECURITY para el valor del sistema de nivel de autorización proporcionan registros de auditoría que pueden ayudarle a detectar intentos de introducir un programa de tipo virus en el sistema. En el capítulo 9 y en el Apéndice F de la publicación *iSeries Security Reference* se proporciona más información acerca de los valores de auditoría y las entradas de diario de auditoría.
- Puede utilizar el parámetro Forzar creación (FRCCRT) del mandato Cambiar programa (CHGPGM) para volver a crear cualquier programa que se haya restaurado en el sistema. El sistema utiliza la plantilla del programa para volver a crearlo. Si el objeto de programa se ha cambiado después de compilarlo, el sistema vuelve a crear el objeto cambiado y lo sustituye. Si la plantilla del programa contiene instrucciones bloqueadas (protegidas), el sistema no volverá a crear el programa de forma satisfactoria.
- Puede utilizar el valor del sistema QFRCCVNRST (forzar conversión al restaurar) para volver a crear cualquier programa al restaurarlo en su sistema. El

sistema utiliza la plantilla del programa para volver a crearlo. Este valor del sistema proporciona varias opciones sobre qué programas pueden volver a crearse.

- Puede utilizar el valor del sistema QVFYOBJRST (verificar objetos en restauración) para evitar la restauración de programas que no tengan una firma digital o que no tengan una firma digital válida. Cuando una firma digital no es válida, significa que se ha modificado el programa desde que lo firmó su desarrollador. Existen API que le permiten firmar sus propios programas, archivos de salvar y archivos continuos.

Para obtener más información sobre la firma y cómo puede utilizarse para proteger el sistema ante ataques, consulte "Firma de objetos" en la página 92.

Supervisión de la utilización de autorizaciones adoptadas

En un servidor iSeries, puede crear un programa que adopte la autorización de su propietario. Esto significa que cualquier usuario que ejecute el programa tendrá las mismas autorizaciones (privadas y especiales) que el perfil de usuario propietario del programa.

La autorización adoptada es una herramienta de seguridad de gran utilidad si se utiliza correctamente. En "Mejora del control de acceso a menús con la seguridad de objetos" en la página 51, por ejemplo, se describe cómo se combinan las autorizaciones adoptadas y los menús para ir más allá del control de acceso a los menús. Puede utilizar la autorización adoptada para impedir la modificación de los archivos importantes fuera de los programas de aplicación aprobados al tiempo que se permite la realización de consultas en ellos.

Como administrador de seguridad, debe asegurarse de que la autorización adoptada se utiliza correctamente:

- Los programas deben adoptar la autorización de un perfil de usuario que sólo tenga autorización para realizar las funciones necesarias. Debe tener especial cuidado con los programas que adoptan la autorización de un perfil de usuario que tenga la autorización especial *ALLOBJ o que sea propietario de objetos importantes.
- Los programas que adoptan autorización deben tener funciones limitadas y específicas, y no deben proporcionar la posibilidad de entrar mandatos.
- Los programas que adoptan autorización deben estar protegidos de forma adecuada.
- El uso excesivo de la autorización adoptada puede tener un efecto negativo en el rendimiento del sistema. Para obtener información que le ayude a evitar problemas de rendimiento, revise los diagramas de flujo de comprobación de autorización y las sugerencias para la utilización de la autorización adoptada que se incluye en Capítulo 5 de la publicación *iSeries Security Reference*.

Opciones del menú SECBATCH:
1 *para someter inmediatamente* **40 para utilizar el planificador de trabajos**

Puede utilizar el mandato Imprimir objetos que adoptan (PRTADPOBJ) (opción 21 del menú SECTOOLS) para que le resulte más fácil supervisar la utilización de la autorización adoptada en el sistema.

El informe muestra las autorizaciones especiales del perfil de usuario especificado, los programas que adoptan la autorización del perfil de usuario, así como dispositivos de ASP que utilizan las autorizaciones del perfil. Después de establecer una base de información, puede imprimir regularmente la versión modificada del informe de objetos adoptados. En él figuran los programas nuevos que adoptan autorización y los programas que se han modificado para que adoptasen la autorización desde la última vez que se generó el informe.

Si sospecha que la autorización adoptada se está utilizando de modo incorrecto en el sistema, puede definir el valor del sistema QAUDLVL de modo que incluya *PGMADP. Cuando este valor está activo, el sistema crea una entrada de diario de auditoría cada vez que se arranca o se finaliza un programa que adopta la autorización. La entrada incluye el nombre del usuario que ha arrancado el programa y el nombre del programa.

Limitación de la utilización de autorizaciones adoptadas

Cuando se ejecuta un programa de iSeries, el programa puede utilizar autorización adoptada para tener acceso a objetos de dos maneras distintas:

- El programa en sí puede adoptar la autorización del propietario. Esto se especifica en el parámetro Perfil de usuario (USRPRF) del programa o del programa de servicio.
- El programa puede utilizar (heredar) la autorización adoptada de un programa anterior que aún esté en la pila de llamadas del trabajo. Un programa puede heredar la autorización adoptada de programas anteriores incluso aunque el programa mismo no adopte autorización. El parámetro Utilizar autorización adoptada (USEADPAUT) de un programa o de un programa de servicio controla si el programa hereda la autorización adoptada de los programas anteriores de la pila de programas.

A continuación se proporciona un ejemplo de cómo funciona la utilización de la autorización adoptada de programas anteriores.

Suponga que el perfil de usuario ICOWNER tiene autorización *CHANGE sobre el archivo ITEM y que la autorización de uso público sobre el archivo ITEM es *USE. Ningún otro perfil tiene una autorización definida explícitamente sobre el archivo ITEM. En Tabla 14 se muestran los atributos para tres programas que utilizan el archivo ITEM:

Tabla 14. Ejemplo de Utilizar autorización adoptada (USEADPAUT)

Nombre del programa	Propietario del programa	Valor del USRPRF	Valor del USEADPAUT
PGMA	ICOWNER	*OWNER	*YES
PGMB	ICOWNER	*USER	*YES
PGMC	ICOWNER	*USER	*NO

Ejemplo 1–Adoptar autorización:
1. USERA ejecuta el programa PGMA.
2. El programa PGMA intenta abrir el archivo ITEM con la posibilidad de actualización.

Resultado: El intento es satisfactorio. USERA tiene acceso *CHANGE para el archivo ITEM porque PGMA adopta la autorización de ICOWNER.

Ejemplo 2–Utilizar la autorización adoptada;:
1. USERA ejecuta el programa PGMA.
2. El programa PGMA llama al programa PGMB.
3. El programa PGMB intenta abrir el archivo ITEM con posibilidad de actualización.

Resultado: El intento es satisfactorio. A pesar de que el programa PGMB no adopta autorización (*USRPRF es *USER), permite que se utilice una autorización adoptada anteriormente (*USEADPAUT es *YES). El programa PGMA está todavía en la pila de programas. Por lo tanto USERA obtiene acceso *CHANGE al archivo ITEM porque PGMA adopta la autorización de ICOWNER.

Ejemplo 3–No utilizar la autorización adoptada:
1. USERA ejecuta el programa PGMA.
2. El programa PGMA llama al programa PGMC.
3. El programa PGMC intenta abrir el archivo ITEM con posibilidad de actualización.

Resultado: Anomalía en la autorización. El programa PGMC no adopta la autorización. El programa PGMC tampoco permite la utilización de autorizaciones adoptadas de programas anteriores. A pesar de que PGMA está todavía en la pila de llamadas, su autorización adoptada no se utiliza.

Impedir que programas nuevos utilicen la autorización adoptada

El paso de la autorización adoptada a programas posteriores de la pila proporciona una oportunidad para un programador experto de crear un programa caballo de Troya. El programa caballo de Troya puede apoyarse en programas anteriores de la pila para obtener la autorización que necesita para realizar acciones no permitidas. Para evitarlo, se pueden limitar los usuarios con permiso para crear programas que utilicen la autorización adoptada de programas anteriores.

Al crear un nuevo programa, el sistema establece automáticamente el parámetro USEADPAUT en *YES. Si no quiere que el programa herede autorización adoptada, debe utilizar el mandato Cambiar programa (CHGPGM) o el mandato Cambiar programa de servicio (CHGSRVPGM) para establecer el parámetro USEADPAUT en *NO.

Puede utilizar una lista de autorizaciones y el valor del sistema de uso de autorización adoptada (QUSEADPAUT) para controlar quién puede crear programas que hereden la autorización adoptada (QUSEADPAUT). Al especificar un nombre de lista de autorizaciones en el valor del sistema QUSEADPAUT, el sistema utiliza esta lista de autorizaciones para determinar cómo crear nuevos programas.

Cuando un usuario crea un programa o un programa de servicio, el sistema comprueba la autorización del usuario sobre la lista de autorizaciones. Si el usuario tiene autorización *USE, el parámetro USEADPAUT para el nuevo programa se establece en *YES. Si el usuario no tiene la autorización *USE, el parámetro USEADPAUT se establece en *NO. La autorización del usuario sobre la lista de autorizaciones no puede proceder de una autorización adoptada.

La lista de autorizaciones que se especifique en el valor del sistema QUSEADPAUT controla también si un usuario puede utilizar un mandato CHGxxx para establecer el valor USEADPAUT para un programa o un programa de servicio.

Notas:

1. No es necesario denominar la lista de autorizaciones como QUESADPAUT. Puede crear una lista de autorizaciones con otro nombre. Después especifique dicha lista para el valor del sistema QUSEADPAUT. En los mandatos de este ejemplo, sustituya el nombre por el de su lista de autorización.
2. El valor del sistema QUSEADPAUT no afecta a los programas existentes en el sistema. Utilice el mandato CGHPGM o CHGSRVPGM para establecer el parámetro USEADPAUT para los programas existentes.

Entorno más restrictivo: Si desea que la mayoría de los usuarios creen programas nuevos con el parámetro USEADPAUT establecido en *NO, haga lo siguiente:

1. Para establecer la autorización de uso público para la lista de autorizaciones en *EXCLUDE, teclee lo siguiente:

```
CHGAUTLE AUTL(QUSEADPAUT) USER(*PUBLIC)
    AUT(*EXCLUDE)
```

2. Para configurar usuarios específicos que puedan crear programas que utilicen la autorización adoptada de programas anteriores, teclee lo siguiente:

```
ADDAUTLE AUTL(QUSEADPAUT) USER(nombre-usuario)
    AUT(*USE)
```

Entorno menos restrictivo: Si desea que la mayoría de los usuarios creen programas nuevos con el parámetro USEADPAUT establecido en *YES, haga lo siguiente:

1. Deje la autorización de uso público para la lista de autorizaciones establecida en *USE.
2. Para evitar que determinados usuarios creen programas que utilicen la autorización adoptada de programas anteriores, teclee lo siguiente:

```
ADDAUTLE AUTL(QUSEADPAUT)
         USER(nombre-usuario) AUT(*EXCLUDE)
```

Supervisión de la utilización de programas desencadenantes

DB2 UDB proporciona la posibilidad de asociar programas desencadenantes con archivos de base de datos. La posibilidad de tener programas desencadenantes es común en el mercado para los gestores de bases de datos de alta funcionalidad.

Cuando se asocia un programa desencadenante con un archivo de base de datos, debe especificarse cuándo se ejecutará el programa. Por ejemplo, puede preparar el archivo de pedidos de clientes para que se ejecute un programa desencadenante siempre que se añade un registro al archivo. Cuando el saldo pendiente del cliente sobrepasa el límite de crédito, el programa desencadenante puede imprimir una carta de aviso al cliente y enviar el mensaje al director de créditos.

Los programas desencadenantes son un método eficaz para proporcionar funciones de aplicación y para gestionar la información. Los programas desencadenantes también proporcionan la posibilidad de que alguien malintencionado pueda crear programas “Caballo de Troya” en su sistema. Puede haber un programa destructivo en espera de ejecutarse cuando se produzca un evento determinado en un archivo de bases de datos del sistema.

Nota: El caballo de Troya era un caballo de madera hueco de gran tamaño que estaba lleno de soldados griegos. El caballo fue introducido dentro de las murallas de Troya, los soldados salieron del caballo y lucharon contra los

Troyanos. En el mundo informático, un programa que oculta funciones destructivas a menudo recibe el nombre de ″caballo de Troya″.

Opciones del menú SECBATCH:
27 *para someter inmediatamente* **66** *para utilizar el planificador de trabajos*

Cuando el sistema sale de fábrica, la posibilidad de añadir un programa desencadenante a un archivo de base de datos está restringida. Si gestiona la autorización sobre objeto cuidadosamente, el usuario normal no tendrá autorización suficiente para añadir un programa desencadenante a un archivo de base de datos. (En el Apéndice D de la publicación *iSeries Security Reference* se indican la autorización necesaria o todos los mandatos, incluyendo el mandato Añadir desencadenante de archivos físicos (ADDPFTRG)).

Puede utilizar el mandato Imprimir programas desencadenantes (PRTTRGPGM) para imprimir una lista de todos los programas desencadenantes de una biblioteca determinada o de todas las bibliotecas.

Puede utilizar el informe inicial como base para evaluar los programas desencadenantes que ya existen en el sistema. Después puede imprimir el informe de modificación regularmente para ver si se han añadido nuevos programas desencadenantes en el sistema.

Cuando evalúe los programas desencadenantes, tenga en cuenta lo siguiente:

- Quién ha creado el programa. Puede utilizar el mandato Visualizar descripción de objeto (DSPOBJD) para determinarlo.
- Qué hace el programa. Tendrá que ver el programa fuente o consultar al creador del programa para averiguarlo. Por ejemplo, ¿comprueba el programa desencadenante quién es el usuario? Quizá el programa desencadenante está a la espera de un usuario determinado (QSECOFR) para obtener el acceso a los recursos del sistema.

Después de establecer una base de información, puede imprimir el informe de modificación regularmente para supervisar los nuevos programas desencadenantes que se hayan añadido al sistema.

Búsqueda de programas ocultos

Los programas desencadenantes no son la única forma posible de introducir un caballo de Troya en el sistema. Los programas desencadenantes son un ejemplo de un **programa de salida**. Cuando se produce un evento determinado, tal como la actualización de un archivo en el caso de un programa desencadenante, el sistema ejecuta el programa de salida asociado al evento.

La Tabla 15 en la página 86 describe otros ejemplos de programas de salida que pueden estar en el sistema. Debe utilizar los mismos métodos para evaluar la utilización y el contenido de estos programas de salida que utiliza para programas desencadenantes.

Nota: La Tabla 15 en la página 86 no es una lista completa de los programas de salida posibles.

.

Tabla 15. Programas de salida proporcionados por el sistema

Nombre del programa	Cuándo se ejecuta el programa
Nombre especificado por el usuario en el atributo de red DDMACC.	Cuando un usuario intenta abrir un archivo DDM en el sistema o efectúa una conexión DRDA.
Nombre especificado por el usuario en el atributo de red PCSACC.	Cuando un usuario intenta utilizar las funciones de Client Access mediante Original Clients para acceder a objetos en el sistema.
Nombre especificado por el usuario en el valor del sistema QPWDVLDPGM.	Cuando un usuario ejecuta la función Cambiar contraseña
Nombre especificado por el usuario en el valor del sistema QRMTSIGN.	Cuando un usuario intenta iniciar la sesión de forma interactiva desde un sistema remoto.
QSYS/QEZUSRCLNP	Cuando se ejecuta la función de limpieza automática.
Nombre especificado por el usuario en el parámetro EXITPGM del mandato CHGBCKUP.	Cuando utiliza la función de copia de seguridad de Operation Assistant.
Nombres especificados por el usuario en el mandato CRTPRDLOD.	Antes y después de salvar, restaurar o suprimir el producto creado con el mandato.
Nombre especificado por el usuario en el parámetro DFTPGM del mandato CHGMSGD.	Si se especifica un programa por omisión para un mensaje, el sistema ejecuta el programa cuando se emite el mensaje. Debido al gran número de descripciones de mensaje en un sistema típico, la utilización de programas por omisión es difícil de supervisar. Para evitar que los usuarios públicos añadan programas por omisión para mensajes, considere la posibilidad de establecer la autorización de uso público para archivos de mensajes (objetos *MSGF) en *USE.
Nombre especificado por el usuario en el parámetro FKEYPGM del mandato STREML3270.	Cuando el usuario pulsa una tecla de función durante la sesión de emulación de dispositivo 3270. El sistema devuelve el control a la sesión de emulación de dispositivo 3270 cuando finaliza el programa de salida.
Nombre especificado por el usuario en el parámetro EXITPGM de los mandatos de supervisión del rendimiento.	Para procesar datos recogidos por los mandatos siguientes: STRPFRMON, ENDPFRMON, ADDPFRCOL y CHGPFRCOL. El programa se ejecuta cuando finaliza la recogida de datos.
Nombre especificado por el usuario en el parámetro EXITPGM del mandato RCVJRNE.	Para cada entrada de diario o grupo de entradas de diario que se han leído del diario y receptor de diario especificados.
Nombre especificado por el usuario en la API QTNADDCR.	Durante una operación COMMIT o ROLLBACK.
Nombres especificados por el usuario en la API QHFRGFS.	Para realizar las funciones del sistema de archivos.
Nombre especificado por el usuario en el parámetro SEPPGM de una descripción de dispositivo de impresora.	Para determinar qué imprimir en la página separadora antes o después de un archivo en spool o de un trabajo de impresión.
QGPL/QUSCLSXT	Cuando se cierra un archivo de base de datos para permitir la captura de información de uso del archivo.
Nombre especificado por el usuario en el parámetro FMTSLR de un archivo lógico.	Cuando se graba un registro en una archivo de base de datos y no se incluye un nombre de formato de registro en el programa de lenguaje de alto nivel. El programa selector recibe el registro como entrada, determina el formato de registro utilizado y lo devuelve a la base de datos.
Nombre especificado por el usuario que se especifica en el valor del sistema QATNPGM, el parámetro ATNPGM en un perfil de usuario o el parámetro PGM del mandato SETATNPGM.	Cuando un usuario pulsa la tecla Atención.

Tabla 15. Programas de salida proporcionados por el sistema (continuación)

Nombre del programa	Cuándo se ejecuta el programa
Nombre especificado por el usuario en el parámetro EXITPGM del mandato TRCJOB.	Antes de empezar el procedimiento de Rastreo de trabajo.

En el caso de los mandatos que permiten especificar un programa de salida, debe asegurarse de que el valor por omisión del mandato no se ha cambiado para especificar un programa de salida. También debe asegurarse de que la autorización de uso público para estos mandatos no sea suficiente para cambiar el valor por omisión del mandato. El mandato CHGCMDDFT necesita autorización *OBJMGT para el mandato. El usuario no necesita autorización *OBJMGT para ejecutar un mandato.

Evaluación de los programas de salida registrados

Puede utilizar la función de registro del sistema para registrar programas de salida que deben ejecutarse cuando tienen lugar determinados eventos. Para listar la información de registro en el sistema, teclee `WRKREGINF OUTPUT(*PRINT)`. La Figura 8 muestra un ejemplo del informe:

```
                          Trabajar con Información de Registro
Punto de salida  . . . . . . . . . . . :   QIBM_QGW_NJEOUTBOUND
Formato de punto de salida . . . . . . :   NJE00100
Punto de salida registrado . . . . . . :   *YES
Permitir quitar registro . . . . . . . :   *YES
Núm. máx. de programas de salida . . . :   *NOMAX
Núm. actual de programas de salida . . :   0
Proceso previo para añadir . . . . . . :   *NONE
  Biblioteca . . . . . . . . . . . . . :
  Formato  . . . . . . . . . . . . . . :
Proceso previo para eliminar . . . . . :   *NONE
  Biblioteca . . . . . . . . . . . . . :
  Formato  . . . . . . . . . . . . . . :
Proceso previo para recuperar  . . . . :   *NONE
  Biblioteca . . . . . . . . . . . . . :
```

Figura 8. Trabajar con información de registro - ejemplo

Para cada punto de salida del sistema, el informe muestra si hay programas de salida registrados actualmente. Cuando un punto de salida tiene programas registrados actualmente, puede seleccionar la opción 8 (Visualizar programas) de la versión de pantalla de WRKREGINF para visualizar información acerca de los programas:

```
                                Trabajar con Información de Registro

Teclee opciones, pulse Intro.
   5=Visualizar punto de salida  8=Trabajar con programas de salida

                           Formato
     Punto                 de punto
 Opc de salida             salida    Registrado  Texto
     QIBM_QGW_NJEOUTBOUND  NJE0100     *YES     Entrada de trabajo de red ext
 8   QIBM_QHQ_DTAQ         DTAQ0100    *YES     Servidor de cola de datos
     QIBM_QLZP_LICENSE     LICM0100    *YES     Servidor de gestión de licenc
     QIBM_QMF_MESSAGE      MESS0100    *YES     Servidor de mensajes original
     QIBM_QNPS_ENTRY       ENTR0100    *YES     Servidor de impresión de red
     QIBM_QNPS_SPLF        SPLF0100    *YES     Servidor de impresión de red
     QIBM_QNS_CRADDACT     ADDA0100    *YES     Añadir actividad de descripci
     QIBM_QNS_CRCHGACT     CHGA0100    *YES     Cambiar actividad de descripc
```

Utilice el mismo método para evaluar estos programas de salida que el utilizado para otros programas de salida y programas desencadenantes.

Comprobación de programas planificados

iSeries proporciona numerosos métodos para planificar trabajos para que se ejecuten más tarde, incluyendo el planificador de trabajos. Normalmente estos métodos no representan un riesgo para la seguridad porque el usuario que planifica el trabajo debe tener la misma autorización que se necesita para someter el trabajo a proceso por lotes.

Sin embargo debe comprobar periódicamente los trabajos planificados. Un usuario descontento que ya no esté en la organización puede utilizar este método para planificar un siniestro.

Restricción de las posibilidades de Salvar y Restaurar

La mayoría de los usuarios no necesitan salvar ni restaurar objetos en el sistema. Los mandatos de salvar proporcionan la posibilidad de copiar elementos importantes de la organización a soportes de almacenamiento o a otro sistema. La mayoría de los mandatos de salvar soportan archivos de salvar que pueden enviarse a otro sistema (utilizando el mandato de archivo SNDNETF) sin tener acceso a un soporte de almacenamiento o a un dispositivo de salvar/restaurar.

Los mandatos para restaurar proporcionan la oportunidad de restaurar objetos no autorizados, tales como programas mandatos y archivos en el sistema. También puede restaurar información sin tener acceso a soportes de almacenamiento o a un dispositivo de salvar/restaurar utilizando archivos de salvar. Los archivos de salvar se pueden enviar desde otro sistema utilizando el mandato SNDNETF o utilizando la función FTP.

A continuación se proporcionan sugerencias para restringir las operaciones de salvar y restaurar en el sistema:

- Controle qué usuarios tienen autorización especial *SAVSYS. La autorización especial *SAVSYS permite al usuario salvar y restaurar objetos incluso cuando el usuario no tiene la autorización necesaria sobre los objetos.
- Controle el acceso físico para salvar y restaurar dispositivos.
- Restrinja el acceso a los mandatos de salvar y restaurar. Cuando instale los programas bajo licencia de OS/400, la autorización de uso público para los mandatos RSTxxx es *EXCLUDE. La autorización de uso público para los

mandatos SAVxxx es *USE. Considere la posibilidad de cambiar la autorización de uso público de los mandatos SAVxxx por *EXCLUDE. Limite cuidadosamente los usuarios que autoriza a utilizar los mandatos RSTxxx.

- Utilice el valor del sistema QALWOBJRST para restringir la restauración de programas de estado del sistema, programas que adoptan autorizaciones y objetos que tienen errores de validación.
- Utilice el valor del sistema QVFYOBJRST para controlar la restauración de objetos firmados en el sistema.
- Utilice el valor del sistema QFRCCVNRST para controlar la creación de determinados objetos que se restauran en el sistema.
- Utilice la auditoría de seguridad para supervisar las operaciones de restauración. Incluya *SAVRST en el valor del sistema QAUDLVL e imprima periódicamente registros de auditoría creados por operaciones de restauración. (En el Capítulo 9 y en el Apéndice F de la publicación *iSeries Security Reference* se proporciona información acerca de las operaciones de entradas de auditoría).

Búsqueda de objetos de usuario en bibliotecas protegidas

Todos los trabajos de un servidor iSeries tienen una lista de bibliotecas. Esta lista determina la secuencia en la que el sistema buscará un objeto si no se especifica un nombre de biblioteca con el nombre de objeto. Por ejemplo, cuando llama a un programa sin especificar dónde está el programa, el sistema busca en la lista de bibliotecas por orden y ejecuta la primera copia del programa que localice.

En la publicación *iSeries Security Reference* se proporciona más información acerca de los riesgos de seguridad de las listas de bibliotecas y de los programas de llamada sin nombre de biblioteca (denominado **llamada no cualificada**). También se proporcionan sugerencias para controlar el contenido de las listas de bibliotecas y la capacidad de cambiar las listas de bibliotecas del sistema.

Para que el sistema se ejecute correctamente, ciertas bibliotecas del sistema, como QSYS y QGPL, deben estar en la lista de bibliotecas para cada trabajo. Debe utilizar la autorización sobre objeto para controlar quién puede añadir programas a estas bibliotecas. De este modo se facilita la tarea de impedir que alguien coloque un programa impostor en una de estas bibliotecas con el mismo nombre que un programa que figura después en una biblioteca de la lista de bibliotecas.

También debe evaluar quién tiene autorización sobre el mandato CHGSYSLIBL y supervisar los registros SV del diario de auditoría de seguridad. Un usuario malintencionado podría añadir una biblioteca delante de QSYS en la lista de bibliotecas y hacer que otros usuarios ejecuten mandatos no autorizados con el mismo nombre que los mandatos proporcionados por IBM.

Opciones del menú SECBATCH:
28 *para someter inmediatamente* **67** *para utilizar el planificador de trabajos*

Puede utilizar el mandato Imprimir objetos de usuario (PRTUSROBJ) para imprimir una lista de objetos de usuario (no creados por IBM) que se encuentran en una biblioteca especificada. Después puede evaluar los programas de la lista para determinar quién los ha creado y qué funciones realizan.

Los objetos de usuario que no son programas también pueden representar un riesgo en la seguridad cuando se encuentran en bibliotecas del sistema. Por ejemplo, si un programa graba datos confidenciales en un archivo cuyo nombre no está calificado, es posible engañar al programa para que abra una versión falsa de ese archivo en una biblioteca del sistema.

Capítulo 10. Prevención y detección de intentos de intrusión

Esta información es una recopilación de varios consejos que le ayudarán a detectar posibles riesgos para la seguridad y personas que cometen fechorías.

Seguridad física

La unidad del sistema es una pieza esencial de su organización y representa una vía de acceso potencial a su sistema. Algunos componentes del sistema son de pequeño tamaño y muy valiosos. Debe colocar la unidad del sistema en un lugar vigilado para evitar la sustracción de componentes valiosos del sistema.

La unidad del sistema dispone de un panel de control que permite realizar funciones básicas sin una estación de trabajo. Por ejemplo, puede utilizarlo para realizar estas acciones:

- Parar el sistema.
- Arrancar el sistema.
- Cargar el sistema operativo.
- Arrancar las funciones de servicio.

Todas estas actividades pueden interrumpir el trabajo de los usuarios del sistema. También representan un riesgo de seguridad potencial para el sistema. Puede utilizar la cerradura existente en el sistema para controlar cuándo se pueden realizar estas actividades. Para impedir la utilización del panel de control, coloque la cerradura en la posición Protegido, quite la llave y guárdela en un lugar seguro.

Notas:

1. Si tiene que efectuar IPL remotas o diagnósticos remotos en el sistema, puede que necesite elegir otra posición para la cerradura. El tema de Iniciación del iSeries Information Center proporciona más información sobre las posiciones de la cerradura (consulte “Requisitos e información relacionada” en la página xii para conocer más detalles).
2. No todos los modelos de sistema incorporan una cerradura como característica estándar.

Supervisión de la actividad de perfiles de usuario

Los perfiles de usuario proporcionan entrada al sistema. Los parámetros del perfil de usuario determinan el entorno y las características de seguridad de un usuario. Como administrador de seguridad, debe controlar y comprobar las modificaciones que se producen en los perfiles de usuario del sistema.

Puede establecer comprobaciones de seguridad para que el sistema grabe un registro de las modificaciones en los perfiles de usuario. Puede utilizar el mandato DSPAUDJRNE para imprimir un informe de estos cambios.

Puede crear programas de salida para evaluar las acciones solicitadas para los perfiles de usuario. La Tabla 16 en la página 92 muestra los puntos de salida disponibles para los mandatos de perfil de usuario.

Tabla 16. Puntos de salida para la actividad de perfil de usuario

Mandato de perfil de usuario	Nombre del punto de salida
Crear perfil de usuario (CRTUSRPRF)	QIBM_QSY_CRT_PROFILE
Cambiar perfil de usuario (CHGUSRPRF)	QIBM_QSY_CHG_PROFILE
Suprimir perfil de usuario (DLTUSRPRF)	QIBM_QSY_DLT_PROFILE
Restaurar perfil de usuario (RSTUSRPRF)	QIBM_QSY_RST_PROFILE

El programa de salida, por ejemplo, puede buscar las modificaciones que pudiesen hacer que el usuario ejecutara una versión no autorizada de un programa. Estas modificaciones podrían ser la asignación de una descripción de trabajo distinta o de una nueva biblioteca actual. Su programa de salida puede notificarlo a una cola de mensajes, o realizar alguna acción (como cambiar o inhabilitar el perfil de usuario) basándose en la información que el programa de salida recibe.

La publicación *iSeries Security Reference* proporciona información acerca de los programas de salida para las acciones de perfil de usuario.

Firma de objetos

Todas las precauciones de seguridad que tome no servirán de nada si alguien puede eludirlas introduciendo datos corruptos en el sistema. El servidor iSeries tiene diversas características incorporadas que puede utilizar para evitar que se cargue software corrupto en su sistema y para detectar si ya hay software de ese tipo. Una de las técnicas añadidas en la V5R1 es la firma de objetos.

La firma de objetos es la implementación en el servidor iSeries de un concepto criptográfico conocido como ″firmas digitales.″ La idea es relativamente sencilla: una vez un productor de software está listo para enviar software a los clientes, el productor ″firma″ el software. Esta firma no garantiza que el software realice ninguna función específica. Sin embargo, proporciona un método para probar que el software proviene del productor que lo ha firmado y que ese software no ha cambiado desde que se generó y se firmó. Esto es de especial importancia si el software se ha transmitido por Internet o se ha almacenado en un soporte que pudiera haber sido modificado.

Utilizar firmas digitales le dará un mayor control sobre qué software puede cargarse en su sistema y le otorgará más poder para detectar cambios una vez cargado. El nuevo valor del sistema Verificar restauración de objeto (QVFYOBJRST) proporciona un mecanismo para establecer una política restrictiva que requiere que todo el software que se cargue en el sistema esté firmado por las fuentes de software conocidas. También puede elegir una política más abierta y simplemente verificar las firmas si las hay.

Todo el software de OS/400, así como el software para las opciones y los programas bajo licencia del servidor iSeries están firmados por una fuente de confianza del sistema. Estas firmas ayudan al sistema a proteger su propia integridad y se comprueban cuando se aplican arreglos al sistema para asegurarse de que el arreglo proviene de una fuente de confianza del sistema y que no ha cambiado por el camino. Estas firmas también pueden comprobarse una vez el software esté en el sistema. El mandato CHKOBJITG (Comprobar integridad de objeto) se ha ampliado para comprobar las firmas, además de otras características de integridad de los objetos en el sistema. Adicionalmente, el Gestor de certificados digitales tiene paneles que puede utilizar para comprobar las firmas de los objetos, incluidos los objetos del sistema operativo.

Estando el sistema operativo firmado, podría igualmente utilizar firmas digitales para proteger la integridad del software que sea vital para su empresa. Podría comprar software que esté firmado por un proveedor de software, o bien podría firmar el software que haya adquirido o escrito. Parte de su política de seguridad sería entonces utilizar CHKOBJITG periódicamente, o el Gestor de certificados digitales, para verificar que las firmas de ese software siguen siendo válidas, es decir, que los objetos no han cambiado desde que se firmaron. Podría ser necesario también que todo el software que se restaure en el sistema esté firmado por usted mismo o por una fuente conocida. Sin embargo, dado que la mayoría del software del servidor iSeries que no ha producido IBM no está firmado, podría resultar demasiado restrictivo para el sistema. El nuevo soporte de firma digital le ofrece flexibilidad para decidir el mejor método para proteger la integridad del software.

Las firmas digitales que protegen el software son tan solo uno de los usos de los certificados digitales. Encontrará información adicional sobre la gestión de certificados digitales en el tema sobre gestión de certificados digitales del Information Center (consulte “Requisitos e información relacionada” en la página xii para conocer más detalles).

Supervisión de descripciones de subsistema

Al arrancar un subsistema en un servidor iSeries, el sistema crea un entorno para que el trabajo entre y se ejecute en el sistema. Una descripción de subsistema define el aspecto que tiene dicho entorno. Por tanto, las descripciones de subsistema pueden ofrecer la oportunidad de entrar al sistema a usuarios con intenciones poco fiables. Estos podrían utilizar una descripción de subsistema para arrancar automáticamente un programa o bien para iniciar una sesión sin un perfil de usuario.

Al ejecutar el mandato Revocar autorización de uso público (RVKPUBAUT), el sistema establece en *EXCLUDE la autorización de uso público para los mandatos de descripción de subsistemas. Con ello se previene que los usuarios que no tienen una autorización específica (y que no tienen autorización especial *ALLOBJ) cambien o creen descripciones de subsistema.

En los temas siguientes se proporcionan sugerencias para revisar las descripciones de subsistema que existen actualmente en el sistema. Puede utilizar el mandato Trabajar con descripciones de subsistema (WRKSBSD) para crear una lista de todas las descripciones de subsistema. Al seleccionar 5 (Visualizar) de la lista, aparecerá un menú para la descripción de sistema seleccionada. Muestra una lista de los componentes de un entorno de subsistema.

Seleccione las opciones para ver detalles acerca de los componentes. Utilice el mandato Cambiar descripción de subsistema (CHGSBSD) para modificar las dos primeras opciones del menú. Para modificar otros elementos, utilice el mandato de añadir, eliminar o modificar (según sea apropiado) para el tipo de entrada. Por ejemplo, para modificar una entrada de estación de trabajo, utilice el mandato Cambiar entrada de estación de trabajo (CHGWSE).

La publicación *Work Management* proporciona más información acerca del trabajo con descripciones de subsistema. También lista los valores iniciales para las descripciones de subsistema suministradas por IBM.

Entradas de trabajo de arranque automático

Una entrada de trabajo de arranque automático contiene el nombre de una descripción de trabajo. La descripción de trabajo puede contener datos de solicitud (RQSDTA) que hacen que un programa o un mandato se ejecute. Por ejemplo, RQSDTA podría ser `CALL LIB1/PROGRAM1`. Siempre que se arranque el subsistema, el sistema ejecutará el programa PROGRAM1 en la biblioteca LIB1.

Consulte las entradas de trabajo de arranque automático y las descripciones de trabajo asociadas. Asegúrese de que entiende el funcionamiento de cualquier programa que se ejecuta automáticamente cuando se arranca un subsistema.

Nombres de estación de trabajo y tipos de estación de trabajo

Cuando se arranca un subsistema, éste asigna todas las estaciones de trabajo no asignadas que figuran (específica o genéricamente) en sus entradas de nombres y tipos de estaciones de trabajo. Cuando un usuario inicia la sesión, se conecta al subsistema que ha asignado la estación de trabajo.

La entrada de estación de trabajo indica qué descripción de trabajo se utilizará cuando se inicia un trabajo en dicha estación de trabajo. La descripción de trabajo puede contener los datos de solicitud que hacen que se ejecute un programa o un mandato. Por ejemplo, el parámetro RQSDTA podría ser `CALL LIB1/PROGRAM1`. Siempre que un usuario inicia la sesión en una estación de trabajo de este subsistema, el sistema ejecutará PROGRAM1 en LIB1.

Consulte las entradas de estación de trabajo y las descripciones de trabajo asociadas. Asegúrese de que nadie ha añadido o actualizado ninguna entrada para ejecutar programas de los que no se tiene conocimiento.

Una entrada de estación de trabajo también podría especificar un perfil de usuario por omisión. Para ciertas configuraciones de subsistema, ello permite que alguien inicie la sesión simplemente pulsando la tecla Intro. Si el nivel de seguridad (valor de sistema QSECURITY) del sistema es inferior a 40, debe revisar las entradas de estación de trabajo para los usuarios por omisión.

Entradas de cola de trabajos

Cuando se arranca un subsistema, éste asigna las colas de trabajos no asignadas que están listadas en la descripción de subsistema. Las entradas de cola de trabajos no constituyen un riesgo directo para la seguridad. Sin embargo, sí proporcionan una oportunidad para que alguien manipule el rendimiento del sistema haciendo que los trabajos se ejecuten en entornos no previstos.

Debe revisar periódicamente las entradas de cola de trabajos en las descripciones de subsistema para asegurarse de que los trabajos por lotes se ejecutan donde deben ejecutarse.

Entradas de direccionamiento

Una entrada de direccionamiento define lo que hace un trabajo cuando entra en el subsistema. Este utiliza entradas de direccionamiento para todos los tipos de trabajos: por lotes, interactivos y de comunicaciones. Una entrada de direccionamiento especifica lo siguiente:

- La clase de trabajo. Al igual que las entradas de cola de trabajos, la clase que está asociada a un trabajo puede afectar a su rendimiento pero no representa un riesgo para la seguridad.
- El programa que se ejecuta cuando se inicia el trabajo. Consulte las entradas de direccionamiento y asegúrese de que nadie ha añadido o actualizado ninguna entrada para ejecutar programas de los que no se tiene conocimiento.

Entradas de comunicaciones y nombres de ubicaciones remotas

Cuando un trabajo de comunicaciones entra en el sistema, éste utiliza las entradas de comunicaciones y las entradas de nombre de ubicación remota del subsistema activo para determinar cómo se ejecutará el trabajo de comunicaciones. Tenga en cuenta lo siguiente respecto a estas entradas:

- Todos los subsistemas son capaces de ejecutar trabajos de comunicaciones. Si un subsistema que está destinado para comunicaciones no está activo, un trabajo que esté intentando entrar en el sistema podría encontrar una entrada en otra descripción de subsistema que satisfaga sus necesidades. Debe examinar las entradas en todas las descripciones de subsistema.
- Una entrada de comunicaciones contiene una descripción de trabajo. La descripción de trabajo puede contener datos de solicitud que ejecutan un mandato o programa. Consulte las entradas de comunicaciones y las descripciones de trabajo asociadas para asegurarse de que entiende cómo se inician los trabajos.
- Una entrada de comunicaciones también especifica un perfil de usuario por omisión que el sistema utiliza en algunas situaciones. Asegúrese de que entiende la función de los perfiles por omisión. Si el sistema contiene perfiles por omisión, debe asegurarse de que tienen una autorización mínima. Consulte el Capítulo 12, “Protección de las comunicaciones APPC” para obtener más información acerca de los perfiles de usuario por omisión.

  Puede utilizar el mandato Imprimir descripción de subsistema (PRTSBSDAUT) para identificar las entradas de comunicaciones que especifican un nombre de perfil de usuario.

Entradas de trabajo de prearranque

Puede utilizar las entradas de trabajo de prearranque para preparar un subsistema para ciertos tipos de trabajos con el fin de que los trabajos se inicien más deprisa. Los trabajos de prearranque pueden iniciarse cuando se arranca el subsistema o cuando sean necesarios. Una entrada de trabajo de prearranque especifica lo siguiente:

- Un programa para ejecutar

  Un perfil de usuario por omisión

  Una descripción de trabajo

Todos ellos tienen riesgos potenciales para la seguridad. Debe asegurarse de que las entradas de trabajo de prearranque sólo realizan funciones autorizadas y previstas.

Trabajos y descripciones de trabajo

Las descripciones de trabajo contienen datos de solicitud y datos de direccionamiento que pueden hacer que se ejecute un programa específico al utilizar dicha descripción de trabajo. Cuando la descripción de trabajo especifica un programa en el parámetro de datos de solicitud, el subsistema ejecuta el

programa. Cuando la descripción de trabajo especifica datos de direccionamiento, el sistema ejecuta el programa especificado en la entrada de direccionamiento que coincide con los datos de direccionamiento.

El sistema utiliza descripciones de trabajo tanto para los trabajos interactivos como para los trabajos por lotes. Para los trabajos interactivos, la entrada de estación de trabajo especifica la descripción de trabajo. Normalmente, el valor de entrada de estación de trabajo es *USRPRF, de modo que el sistema utiliza la descripción de trabajo especificada en el perfil de usuario. Para los trabajos por lotes, el usuario especifica la descripción de trabajo al someter el trabajo.

Debe revisar periódicamente las descripciones de trabajo para asegurarse de que éstas no ejecutan programas no previstos. También debe utilizar la autorización sobre objeto para evitar modificaciones en las descripciones de trabajo. La autorización *USE es suficiente para ejecutar un trabajo con una descripción de trabajo. Un usuario típico no necesita autorización *CHANGE para las descripciones de trabajo.

Opciones del menú SECBATCH:
15 *para someter inmediatamente* **54** *para utilizar el planificador de trabajos*

Las descripciones de trabajo también pueden especificar bajo qué perfil de usuario se debe ejecutar el trabajo. Con el nivel de seguridad 40 y superior, debe tener autorización *USE para la descripción de trabajo y para el perfil de usuario especificados en la descripción de trabajo. Con los niveles de seguridad inferiores a 40, sólo se necesita autorización *USE para la descripción de trabajo.

Puede utilizar el mandato Imprimir autorización de descripción de trabajo (PRTJOBDAUT) para imprimir una lista de descripciones de trabajos que especifican perfiles de usuario y cuya autorización de uso público es *USE.

El informe muestra las autorizaciones especiales del perfil de usuario especificado en la descripción de trabajo. El informe incluye las autorizaciones especiales de cualquier perfil de grupo que el perfil de usuario tenga. Puede utilizar el siguiente mandato para visualizar las autorizaciones privadas del perfil de usuario ':

```
DSPUSRPRF USRPRF(nombre perfil) TYPE(*OBJAUT)
```

La descripción de trabajo especifica la lista de bibliotecas que utiliza el trabajo cuando se ejecuta. Si alguien puede modificar una lista de bibliotecas de un usuario, dicho usuario podría ejecutar una versión no prevista de un programa en una biblioteca diferente. Debe revisar periódicamente las listas de bibliotecas especificadas en las descripciones de trabajo del sistema.

Finalmente, debe asegurarse de que los valores por omisión para el mandato Someter trabajo (SBMJOB) y el mandato Crear perfil de usuario (CRTUSRPRF) no se han modificado para que apunten a descripciones de trabajo no previstas.

Nombres de programas de transacciones con arquitectura

Algunas peticiones de comunicaciones envían un tipo específico de señal al sistema. Esta petición se llama **nombre de programa de transacciones con arquitectura (TPN)** ya que el nombre del programa de transacciones forma parte de la arquitectura APPC del sistema. Una petición de paso a través de estación de

pantalla es un ejemplo de un TPN con arquitectura. Los TPN con arquitectura son un procedimiento normal para que funcionen las comunicaciones y no necesariamente representan un riesgo para la seguridad. Sin embargo, los TPN con arquitectura pueden proporcionar una entrada inesperada al sistema.

Algunos TPN no pasan ningún perfil en la petición. Si la petición llega a asociarse con una entrada de comunicaciones cuyo usuario por omisión es *SYS, la petición puede iniciarse en el sistema. Sin embargo, el perfil *SYS sólo puede ejecutar funciones del sistema y no aplicaciones de usuario.

Si no desea que los TPN con arquitectura se ejecuten con un perfil por omisión, puede modificar el usuario por omisión de *SYS a *NONE en las entradas de comunicaciones. En la "Peticiones de TPN con arquitectura" se indican los TPN con arquitectura y los perfiles de usuario asociados.

Si no desea que un TPN específico se ejecute en el sistema, realice las siguientes acciones:

1. Cree un programa CL que acepte varios parámetros. El programa no debe realizar ninguna función. Simplemente debe tener las sentencias Declarar (DCL) para los parámetros y después finalizar.
2. Añada una entrada de direccionamiento para el TPN a cada subsistema que tenga entradas de comunicaciones o entradas de nombre de ubicación remota. La entrada de direccionamiento debe especificar lo siguiente:
   - Un valor *Comparar valor* (CMPVAL) igual al nombre del programa del TPN (consulte Peticiones de TPN con arquitectura) con una posición inicial de 37.
   - Un valor *Programa a llamar* (PGM) igual al nombre del programa creado en el paso 1. Ello impide que el TPN ubique otra entrada de direccionamiento, como por ejemplo *ANY.

Varios TPN ya tienen su propia entrada de direccionamiento en el subsistema QCMN. Se han añadido por motivos de rendimiento.

Peticiones de TPN con arquitectura

Tabla 17. Programas y usuarios para peticiones de TPN

Petición de TPN	Programa	Perfil de usuario	Descripción
X'30F0F8F1'	AMQCRC6A	*NONE	Cola de mensajes
X'06F3F0F1'	QACSOTP	QUSER	Programa de transacciones de inicio de sesión APPC
X'30F0F2D1'	QANRTP	QADSM	Configuración ADSM/400 APPC
X'30F0F1F9'	QCNPCSUP	*NONE	Carpetas compartidas
X'07F0F0F1'	QCNTEDDM	QUSER	DDM
X'07F6C4C2'	QCNTEDDM	QUSER	SQL–DRDA1 remoto
X'30F0F7F7'	QCQNRBAS	QSVCCS	Servidor CC_ de SNA
X'30F0F1F4'	QDXPRCV	QUSER	Receptor de DSNX–PC
X'30F0F1F3'	QDXPSEND	QUSER	Emisor de DSNX–PC
X'30F0F2C4'	QEVYMAIN	QUSER	Servidor ENVY**/400
X'30F0F6F0'	QHQTRGT	*NONE	Cola de datos en PC
X'30F0F8F0'	QLZPSERV	*NONE	Gestor de licencias Client Access
X'30F0F1F7'	QMFRCVR	*NONE	Receptor de mensajes en PC

Tabla 17. Programas y usuarios para peticiones de TPN (continuación)

Petición de TPN	Programa	Perfil de usuario	Descripción
X'30F0F1F8'	QMFSNDR	*NONE	Emisor de mensajes en PC
X'30F0F6F6'	QND5MAIN	QUSER	Controlador de estación de trabajo APPN 5394
DB2DRDA	QCNTEDDDM	QUSER	DB2DRDA
APINGD	QNMAPINGD	QUSER	APINGD
X'30F0F5F4'	QNMEVK	QUSER	Programas de utilidad de gestión del sistema
X'30F0F2C1'	QNPSERVR	*NONE	Servidor de impresión de red PWS-I
X'30F0F7F9'	QOCEVOKE	*NONE	Calendario de sistemas cruzados
X'30F0F6F1'	QOKCSUP	QDOC	Duplicación de directorio
X'20F0F0F7'	QOQSESRV	QUSER	DIA Versión 2
X'20F0F0F8'	QOQSESRV	QUSER	DIA Versión 2
X'30F0F5F1'	QOQSESRV	QUSER	DIA Versión 2
X'20F0F0F0'	QOSAPPC	QUSER	DIA Versión 1
X'30F0F0F5'	QPAPAST2	QUSER	Paso a través de S/36—S/38
X'30F0F0F9'	QPAPAST2	QUSER	Paso a través de impresora
X'30F0F4F6'	QPWFSTP0	*NONE	Carpetas compartidas Tipo 2
X'30F0F2C8'	QPWFSTP1	*NONE	Servidor de archivos de Client Access
X'30F0F2C9'	QPWFSTP2	*NONE	Servidor de archivos de Windows** Client Access
X'30F0F6F9'	QRQSRVX	*NONE	SQL remoto – servidor convergente
X'30F0F6F5'	QRQSRV0	*NONE	SQL remoto sin compromiso
X'30F0F6F4'	QRQSRV1	*NONE	SQL remoto sin compromiso
X'30F0F2D2'	QSVRCI	QUSER	SOC/CT
X'21F0F0F8'	QS2RCVR	QGATE	Receptor SNADS FS2
X'21F0F0F7'	QS2STSND	QGATE	Emisor SNADS FS2
X'30F0F1F6'	QTFDWNLD	*NONE	Función de transferencia de PC
X'30F0F2F4'	QTIHNPCS	QUSER	Función TIE
X'30F0F1F5'	QVPPRINT	*NONE	Impresión virtual en PC
X'30F0F2D3'	QWGMTP	QWGM	Ultimedia Mail/400 Server
X'30F0F8F3'	QZDAINIT	QUSER	Servidor de acceso a datos PWS-I
X'21F0F0F2'	QZDRCVR	QSNADS	Receptor SNADS
X'21F0F0F1'	QZDSTSND	QSNADS	Emisor SNADS
X'30F0F2C5'	QZHQTRG	*NONE	Servidor de cola de datos PWS-I
X'30F0F2C6'	QZRCSRVR	*NONE	Servidor de mandatos remotos PWS-I
X'30F0F2C7'	QZSCSRVR	*NONE	Servidor central PWS-I

Métodos para supervisar eventos de seguridad

La puesta a punto de la seguridad no es un esfuerzo que se haga de una sola vez. Es necesario evaluar constantemente los cambios en el sistema y las anomalías en la seguridad. Después hay que realizar ajustes en el entorno de seguridad que respondan a lo que se ha descubierto.

Los informes de seguridad le ayudan a supervisar los cambios relativos a la seguridad que se producen en el sistema. A continuación se indican otras funciones del sistema que puede utilizar para ayudarle a detectar anomalías o riesgos para la seguridad:

- La auditoría de seguridad es una herramienta potente que puede utilizar para observar diferentes tipos de eventos relativos a la seguridad que se producen en el sistema. Por ejemplo, puede poner a punto el sistema para que grabe un registro de auditoría cada vez que un usuario abra un archivo de base de datos para actualizarlo. Puede hacer una auditoría de todos los cambios efectuados en los valores del sistema. Puede hacer una auditoría de las acciones que ocurren cuando los usuarios restauran objetos.

  En el Capítulo 9 de la publicación *iSeries Security Reference* se proporciona información completa acerca de la función de auditoría de seguridad. Puede utilizar el mandato Cambiar auditoría de seguridad (CHGSECAUD) para poner a punto la auditoría de seguridad en el sistema. También puede utilizar el mandato Visualizar entradas de diario de auditoría (DSPAUDJRNE) para imprimir información seleccionada del diario de auditoría de seguridad.
- Puede crear la cola de mensajes QSYSMSG para capturar mensajes críticos del operador del sistema. La cola de mensajes QSYSOPR recibe muchos mensajes de diversa importancia durante un día normal de trabajo. Los mensajes críticos relativos a la seguridad pueden pasarse por alto debido al gran volumen de mensajes que hay en la cola de mensajes QSYSOPR.

  Si se crea una cola de mensajes QSYSMSG en la biblioteca QSYS del sistema, este dirige automáticamente ciertos mensajes críticos a la cola de mensajes QSYSMSG en lugar de a la cola de mensajes QSYSOPR.

  Puede crear un programa para supervisar la cola de mensajes QSYSMSG o bien puede asignarla en la modalidad de interrupción para usted mismo o para otro usuario de confianza.

Parte 3. Aplicaciones y comunicaciones de red

Capítulo 11. Utilización del Sistema de Archivos Integrado (IFS) para proteger archivos

El sistema de archivos integrado le proporciona múltiples formas de almacenar y ver información en el servidor iSeries. Este sistema de archivos integrado forma parte del sistema operativo de OS/400 que ofrece soporte para operaciones de entrada y salida continuas. Proporciona métodos de gestión de almacenamiento similares a (y compatibles con) los sistemas operativos de PC y sistemas operativos UNIX.

Con el sistema de archivos integrado, todos los objetos del sistema se pueden ver al mismo tiempo desde la perspectiva de una estructura de directorios jerárquica. Sin embargo, en muchos casos, los usuarios ven los objetos del modo más común para un sistema de archivos determinado. Por ejemplo, los objetos de iSeries ″tradicionales″ se encuentran en el sistema de archivos QSYS.LIB. Por lo general, los usuarios ven los objetos desde la perspectiva de bibliotecas. Los usuarios visualizan los objetos del sistema de archivos QDLS desde la perspectiva de documentos dentro de carpetas. Los sistemas de archivos raíz (/), QOpenSys y los definidos por el usuario presentan una estructura de directorios jerárquicos (anidados).

Como administrador de seguridad debe conocer lo siguiente:

- Qué sistemas de archivos se utilizan en el sistema
- Las características de seguridad exclusivas de cada sistema de archivos

En los temas siguientes se proporcionan algunas consideraciones generales acerca de la seguridad del sistema de archivos integrado.

El método de seguridad del Sistema de Archivos Integrado (IFS)

El sistema de archivos raíz actúa como la base (o los cimientos) para todos los demás sistemas de archivos en los servidores iSeries. En un nivel superior, proporciona una vista integrada de todos los objetos del sistema. Otros sistemas de archivos que puedan existir en los servidores iSeries proporcionan distintas propuestas para la integración y la gestión de objetos, dependiendo de la finalidad básica de cada sistema de archivos. El sistema de archivos QOPT (óptico), por ejemplo, permite a las aplicaciones y los servidores de iSeries (incluido el servidor de archivos iSeries Access para Windows) acceder a la unidad de CD-ROM del servidor iSeries. Del mismo modo, el sistema de archivos QFileSvr.400 permite a las aplicaciones acceder a los datos del sistema de archivos integrado de servidores iSeries remotos. El servidor de archivos QLANSrv permite acceder a los archivos almacenados en el Servidor xSeries Integrado para iSeries o en otros servidores conectados de la red.

La propuesta para la seguridad de cada sistema de archivos depende de los datos que cada sistema de archivos permite que estén disponibles. El sistema de archivos QOPT, por ejemplo, no proporciona seguridad de nivel de objeto, puesto que no existe tecnología para escribir información de autorización en un CD-ROM. Para el sistema de archivos QFileSvr.400, el control de acceso se lleva a cabo en el sistema remoto (donde se gestionan y están almacenados los archivos físicamente). Para los sistemas de archivos como, por ejemplo, QLANSrv, el Servidor xSeries Integrado para iSeries proporciona control de acceso. A pesar de los distintos modelos de

seguridad, muchos sistemas de archivos soportan la gestión coherente del control de acceso a través de los mandatos del sistema de archivos integrado, tales como Cambiar autorización (CHGAUT) y Cambiar propietario (CHGOWN).

Estos son algunos consejos relacionados con todos los aspectos de la seguridad del sistema de archivos integrado. El sistema de archivos integrado está diseñado para seguir los estándares de POSIX con la mayor precisión posible. Esto conduce a un comportamiento interesante, en el que la autorización de servidor iSeries y los permisos de POSIX se ″mezclan″:

1. No elimine la autorización privada de un usuario sobre un directorio propiedad de ese usuario, incluso si el usuario está autorizado mediante la autorización de uso público, un grupo o una lista de autorizaciones. Al trabajar con bibliotecas o carpetas en el modelo de seguridad de servidor iSeries estándar, eliminar la autorización privada del propietario reduciría la cantidad de información sobre autorizaciones almacenada para un perfil de usuario y no afectaría a otras operaciones. De todas maneras, debido a la forma en que el estándar POSIX define la herencia de permisos para directorios, el propietario de un directorio recién creado tendrá las mismas autorizaciones sobre objetos para ese directorio que el propietario del padre tiene sobre el padre, incluso si el propietario del directorio recién creado tiene otras autorizaciones privadas sobre el padre. Para comprenderlo mejor, he aquí un ejemplo: USERA posee el directorio /DIRA, pero se han eliminado las autorizaciones privadas de USERA. USERB tiene autorización privada sobre /DIRA. USERB crea el directorio /DIRA/DIRB. Dado que USERA no tiene autorizaciones sobre objeto en /DIRA, USERB no tendrá autorizaciones sobre objeto en /DIRA/DIRB. USERB no podrá redenominar ni suprimir /DIRA/DIRB sin tener que llevar a cabo acciones para cambiar las autorizaciones sobre objeto de USERB. Esto también entra en juego al crear archivos con la API open() utilizando el distintivo O_INHERITMODE. Si USERB ha creado un archivo /DIRA/FILEB, USERB no tendrá autorizaciones sobre objeto NI autorizaciones de datos sobre él. USERB no podrá grabar en el nuevo archivo.
2. La autorización adoptada no se acepta en la mayoría de sistemas de archivos físicos. Eso incluye los sistemas de archivos raíz (/), QOpenSys, QDLS y los definidos por el usuario.
3. Los objetos existentes son propiedad del perfil de usuario que los haya creado, incluso si el campo OWNER del perfil de usuario está establecido como *GRPPRF.
4. Muchas operaciones del sistema de archivos requieren autorización de datos *RX para cada componente de la vía de acceso, incluido el directorio raíz (/). Al experimentar problemas con las autorizaciones, asegúrese de comprobar la autorización del usuario sobre el propio directorio raíz.
5. Visualizar o recuperar el directorio de trabajo actual (DSPCURDIR, getcwd(), etc.) requiere autorización de datos *RX para cada componente de la vía de acceso. No obstante, modificar el directorio de trabajo actual (CD, chdir(), etc.) solamente requiere autorización de datos *X para cada componente. Por consiguiente, un usuario puede cambiar el directorio de trabajo actual a una vía de acceso determinada y luego no poder visualizar esa vía de acceso.
6. La finalidad del mandato COPY es duplicar un objeto. Los valores de autorización en el nuevo archivo serán los mismos que en el original, excepto el propietario. La finalidad del mandato CPYTOSTMF, no obstante, es simplemente duplicar datos. El usuario no puede controlar los valores de autorización en el nuevo archivo. El creador/propietario tendrá autorización de datos *RWX, pero las autorizaciones de uso público y de grupo serán

*EXCLUDE. El usuario debe utilizar otros medios (CHGAUT, chmod(), etc.) para asignar las autorizaciones deseadas.

7. Un usuario debe ser el propietario o tener autorización sobre objeto *OBJMGT para recuperar información de autorización sobre un objeto. Esto puede aparecer en lugares inesperados, como COPY, que debe recuperar la información de autorización del objeto origen para establecer las autorizaciones equivalentes en el objeto destino.
8. Al cambiar el propietario o el grupo de un objeto, el usuario no debe tener solamente la autorización adecuada sobre el objeto, sino que también debe tener la autorización de datos *ADD sobre el nuevo perfil de usuario de propietario/grupo y la autorización de datos *DELETE sobre el antiguo perfil de propietario/grupo. Estas autorizaciones de datos no están relacionadas con las autorizaciones de datos del sistema de archivos. Estas autorizaciones de datos pueden visualizarse utilizando el mandato DSPOBJAUT y modificarse utilizando el mandato EDTOBJAUT. Esto también puede aparecer inesperadamente en COPY cuando intenta definir el ID de grupo para un objeto nuevo.
9. El mandato MOV tiene tendencia a sufrir errores de autorización extraños, especialmente al trasladar de un sistema de archivos físico a otro o al realizar conversión de datos. En estos casos, el traslado se convierte realmente en una operación de copiar y suprimir. Por consiguiente, el mandato MOV puede resultar afectado por las mismas consideraciones sobre autorizaciones que el mandato COPY (vea los puntos 7 y 8) y el mandato RMVLNK, aparte de otras consideraciones específicas de MOV.

Los apartados siguientes ofrecen consideraciones sobre diversos sistemas de archivos representativos. Para obtener más información acerca de un sistema de archivos específico de su servidor iSeries, debe consultar la documentación correspondiente al programa bajo licencia que utiliza el sistema de archivos.

Sistemas de archivos raíz (/), QOpenSys y definidos por usuario

A continuación se presentan algunas consideraciones sobre la seguridad para los sistemas de archivos raíz, QOpenSys y los definidos por el usuario.

Cómo funcionan las autorizaciones

Los sistemas de archivos raíz, QOpenSys y los definidos por el usuario proporcionan una combinación de las posibilidades del servidor iSeries, PC y UNIX** tanto para la gestión de objetos como para la seguridad. Al utilizar los mandatos del sistema de archivos integrado de una sesión del servidor iSeries (WRKAUT y CHGAUT), puede establecer todas las autorizaciones de objeto de servidor iSeries normales. Esto incluye las autorizaciones *R, *W y *X que son compatibles con Spec 1170 (sistemas operativos de tipo UNIX).

Nota: Los sistemas de archivos raíz, QOpenSys y los definidos por el usuario son equivalentes en sus funciones. El sistema de archivos QOpenSys es sensible a las mayúsculas y el sistema de archivos raíz no. Los sistemas de archivos definidos por el usuario pueden definirse como sensibles a las mayúsculas y minúsculas. Dado que estos sistemas de archivos tienen las mismas características de seguridad, en los temas siguientes se puede dar por supuesto que sus nombres se utilizan indistintamente.

Al acceder al sistema de archivos raíz como administrador desde una sesión de PC, puede establecer los atributos de objetos que utiliza el PC para restringir determinados tipos de acceso:

- Sistema
- Ocultar
- Archivar
- Sólo lectura

Estos atributos del PC se añaden y no sustituyen a los valores de autorización sobre objeto del servidor iSeries.

Cuando un usuario intenta acceder a un objeto del sistema de archivos raíz, el OS/400 aplica todos los atributos y valores de autorización para el objeto, tanto si dichas autorizaciones son ″visibles″ desde la interfaz del usuario como si no. Por ejemplo, suponga que el atributo de sólo lectura para un objeto está activado. Un usuario de PC no puede suprimir el objeto a través de una interfaz de iSeries Access. Un usuario de servidor iSeries con una estación de trabajo de función fija tampoco puede suprimir el objeto incluso aunque el usuario del servidor iSeries tenga autorización especial *ALLOBJ. Para eliminar el objeto, un usuario autorizado debe utilizar una función de PC para restablecer el valor de sólo lectura en `desactivado`. Del mismo modo, un usuario de PC puede no tener la autorización de OS/400 suficiente para cambiar los atributos de seguridad relacionados con el PC de un objeto.

Las aplicaciones de tipo UNIX que se ejecutan en servidores iSeries utilizan interfaces de programación de aplicaciones (API) de tipo UNIX para acceder a los datos del sistema de archivos raíz. Con API de tipo UNIX, las aplicaciones pueden reconocer y mantener la información de seguridad siguiente:
- Propietario de objeto
- Propietario de grupo (autorización de grupo primario de servidor iSeries)
- Lectura (archivos)
- Escritura (modificar el contenido)
- Ejecución (ejecutar programas o buscar directorios)

El sistema correlaciona estas autorizaciones de datos con las autorizaciones de datos y objetos existentes del servidor iSeries:
- Lectura (*R) = *OBJOPR y *READ
- Escritura (*W) = *OBJOPR, *ADD, *UPD, *DLT
- Ejecución (*X) = *OBJOPR y *EXECUTE

Los conceptos de otras autorizaciones sobre objeto (*OBJMGT, *OBJEXIST, *OBJALTER y *OBJREF) no existen en un entorno de tipo UNIX.

Sin embargo, estas autorizaciones sobre objeto existen para todos los objetos del sistema de archivos raíz. Al crear un objeto utilizando una API de tipo UNIX, ese objeto hereda estas autorizaciones del directorio padre, dando como resultado lo siguiente:
- El propietario del objeto nuevo tiene la misma autorización sobre objeto que el propietario del directorio padre.
- El grupo primario del objeto nuevo tiene la misma autorización sobre objeto que el grupo primario del directorio padre.
- El público del objeto nuevo tiene la misma autorización sobre objeto que el público del directorio padre.

La autorización sobre datos del objeto nuevo para propietario, grupo primario y público se especifica en la API con el parámetro de modalidad. Cuando todas las autorizaciones sobre objeto están establecidas como 'activadas', obtendrá el mismo

comportamiento por parte de las autorizaciones que el que esperaría en un entorno de tipo UNIX. Es mejor dejarlas 'activadas', a menos que no desee un comportamiento como el de POSIX.

Al ejecutar aplicaciones que utilizan API de tipo UNIX, el sistema fuerza todas las autorizaciones sobre objeto, tanto si son "visibles" a las aplicaciones UNIX como si no. Por ejemplo, el sistema fuerza la autorización de listas de autorizaciones, aunque en los sistemas operativos de tipo UNIX no exista el concepto de listas de autorizaciones.

Si dispone de un entorno de aplicaciones mixtas, debe asegurarse de que no realiza cambios de autorizaciones en un entorno que pueda interrumpir sus aplicaciones en otro entorno.

Trabajar con la seguridad para los sistemas de archivos raíz (/), QOpenSys y los definidos por usuario

Al introducir el sistema de archivos integrado, los servidores iSeries también proporcionan un nuevo conjunto de mandatos para trabajar con objetos en múltiples sistemas de archivos. En este conjunto se incluyen mandatos para trabajar con la seguridad:

- Cambiar auditoría (CHGAUD)
- Cambiar autorización (CHGAUT)
- Cambiar propietario (CHGOWN)
- Cambiar grupo primario (CHGPGP)
- Visualizar autorización (DSPAUT)
- Trabajar con autorización (WRKAUT)

Estos mandatos agrupan las autorizaciones básicas sobre objeto y sobre datos en subconjuntos de autorizaciones de tipo UNIX.

***RWX** Leer/grabar/ejecutar
***RW** Leer/grabar
***R** Leer
***WX** Grabar/ejecutar
***W** Grabar
***X** Ejecutar

Además, hay interfaces API de tipo UNIX disponibles para trabajar con la seguridad.

Autorización de uso público para el directorio raíz

Al entregar el sistema, la autorización de uso público para el directorio raíz es *ALL (todas las autorizaciones sobre objeto y sobre datos). Este valor proporciona la flexibilidad y la compatibilidad necesarias para ajustarse a las necesidades de las aplicaciones de tipo UNIX y a lo que esperan los usuarios típicos del servidor iSeries. Un usuario del servidor iSeries con la posibilidad de línea de mandatos puede crear una nueva biblioteca en el sistema de archivos QSYS.LIB simplemente utilizando el mandato CRTLIB. Por lo general, la autorización en un servidor iSeries normal lo permite. Del mismo modo, con el valor recibido originalmente para el sistema de archivos raíz, un usuario puede crear un nuevo directorio raíz (del mismo modo que se crea un nuevo directorio en el PC).

Como administrador de seguridad, debe educar a sus usuarios acerca de cómo deben proteger adecuadamente los objetos que crean. Cuando un usuario crea una biblioteca, probablemente la autorización de uso público para la biblioteca no deba

ser *CHANGE (el valor por omisión). El usuario debe establecer la autorización de uso público para *USE o para *EXCLUDE, dependiendo del contenido de la biblioteca.

Si los usuarios necesitan crear directorios nuevos en los sistemas de archivos raíz (/), QOpenSys o los definidos por el usuario, existen diversas opciones de seguridad:

- Puede enseñar a sus usuarios a que alteren temporalmente la autorización por omisión al crear nuevos directorios. El valor por omisión es la herencia de la autorización del directorio padre inmediato. En el caso de un directorio que se acaba de crear en el directorio raíz, la autorización de uso público por omisión será *ALL.
- Puede crear un subdirectorio ″maestro″ bajo el directorio raíz. Establezca la autorización de uso público del directorio maestro en un valor adecuado para su organización y, a continuación, solicite a sus usuarios que creen todos sus directorios personales nuevos en este subdirectorio maestro. Sus nuevos directorios heredarán la autorización.
- Puede cambiar la autorización de uso público para el directorio raíz con el fin de evitar que los usuarios creen objetos en dicho directorio. (Elimine las autorizaciones *W, *OBJEXIST, *OBJALTER, *OBJREF y *OBJMGT.) No obstante, debe evaluar si este cambio puede causar problemas en cualquiera de sus aplicaciones. Por ejemplo, puede tener aplicaciones de tipo UNIX que puedan suprimir objetos del directorio raíz.

Mandato Imprimir objetos con autorización privada (PRTPVTAUT)

Puede utilizar el mandato Imprimir autorización privada (PRTPVTAUT) para imprimir un informe de todas las autorizaciones privadas correspondientes a los objetos de un tipo determinado de una biblioteca, carpeta o directorio especificados. El informe lista todos los objetos del tipo especificado y los usuarios autorizados de dichos objetos. Constituye una forma de comprobar las distintas fuentes de las autorizaciones de los objetos.

Este mandato imprime tres informes de los objetos seleccionados. El primer informe (Informe completo) contiene todas las autorizaciones privadas de todos los objetos seleccionados. El segundo informe (Informe de cambios) contiene adiciones y cambios en las autorizaciones privadas de los objetos seleccionados, si previamente se ha ejecutado el mandato PRTPVTAUT en los objetos especificados de la biblioteca, carpeta o directorio especificados. Todo objeto nuevo, nuevas autorizaciones en objetos existentes o cambios en las autorizaciones existentes de los objetos existentes se listarán en el 'Informe de cambios'. Si previamente no se ha ejecutado el mandato PRTPVTAUT para los objetos especificados en la biblioteca, carpeta o directorio especificados, no se creará ningún 'Informe de cambios'. Si previamente se ha ejecutado el mandato, pero no se han efectuado cambios en las autorizaciones de los objetos, se imprimirá el 'Informe de cambios', aunque no listará ningún objeto.

El tercer informe (Informe de supresiones) contiene todas las supresiones de los usuarios con autorizaciones privadas de los objetos especificados, desde que se ejecutó por última vez el mandato PRTPTVAUT. Todos los objetos suprimidos, o todos los usuarios que se hayan eliminado como usuarios con autorizaciones privadas, se listarán en el 'Informe de eliminaciones'. Si previamente no se ha ejecutado el mandato PRTPTVAUT, no se creará ningún 'Informe de eliminaciones'.

Si previamente se ha ejecutado el mandato, pero no se han efectuado operaciones de supresión en los objetos, se imprimirá el 'Informe de supresiones', aunque no listará ningún objeto.

Restricción: Deberá tener la autorización especial *ALLOBJ para utilizar este mandato.

Ejemplos:

Este mandato crea los informes completo, de cambios y de supresiones para todos los objetos de archivo de PAYROLLLIB:

```
PRTPVTAUT OBJTYPE(*FILE) LIB(PAYROLLLIB)
```

Este mandato crea los informes completo, de cambios y de supresiones para todos los objetos de archivo continuo del directorio garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*NO)
```

Este mandato crea los informes completo, de cambios y de supresiones para todos los objetos de archivo continuo de la estructura de subdirectorios que empieza en el directorio garry:

```
PRTPVTAUT OBJTYPE(*STMF) DIR(/GARRY) SCHSUBDIR(*YES)
```

Mandato Imprimir objetos con autorizaciones de uso público (PRTPUBAUT)

El mandato Imprimir objetos con autorizaciones de uso público (PRTPUBAUT) permite imprimir un informe de los objetos especificados que no posean la autorización de uso público de *EXCLUDE. En los objetos *PGM, solamente los programas que no posean una autorización de uso público de *EXCLUDE que pueda llamar un usuario (el programa es del dominio del usuario, o bien tiene un nivel de seguridad del sistema (valor del sistema QSECURITY) de 30 o inferior), se incluirán en el informe. Constituye una forma de comprobar los objetos que todos los usuarios del sistema están autorizados a acceder.

Este mandato imprimirá dos informes. El primer informe (Informe completo) contendrá todos los objetos especificados que no posean una autorización de uso público de *EXCLUDE. El segundo informe (Informe de cambios) contendrá los objetos que ahora no tengan la autorización de uso público de *EXCLUDE, y que anteriormente tuvieran la autorización de uso público de *EXCLUDE o bien no existieran cuando se ejecutara previamente el mandato PRTPUBAUT. Si no se hubiera ejecutado previamente el mandato PRTPUBAUT para los objetos especificados y la biblioteca, carpeta o directorio, no se creará ningún 'Informe de cambios'. Si se hubiese ejecutado previamente el mandato, pero ningún objeto adicional no tuviera la autorización de uso público de *EXCLUDE, se imprimirá el 'Informe de cambios', aunque no listará ningún objeto.

Restricciones: Deberá tener la autorización especial de *ALLOBJ para utilizar este comando.

Ejemplos:

Este mandato crea los informes completo y de cambios para todos los objetos de archivo de la biblioteca GARRY que no tienen una autorización de uso público *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*FILE) LIB(GARRY)
```

Este mandato crea los informes completo, de cambios y de supresiones para todos los objetos de archivo continuo de la estructura de subdirectorios que empieza en el directorio garry, que no tienen una autorización de uso público *EXCLUDE:

```
PRTPUBAUT OBJTYPE(*STMF) DIR(GARRY) SCHSUBDIR(*YES)
```

Restricción del acceso al sistema de archivos QSYS.LIB

Puesto que el sistema de archivos raíz se considera como el sistema de archivos base, el sistema de archivos QSYS.LIB constituye un subdirectorio dentro del directorio raíz. Por consiguiente, cualquier usuario de PC que disponga de acceso al servidor iSeries puede manipular los objetos almacenados en las bibliotecas del servidor iSeries (el sistema de archivos QSYS.LIB) con acciones y mandatos de PC normales. Un usuario de PC puede, por ejemplo, arrastrar un objeto de QSYS.LIB (como la biblioteca con sus archivos de datos críticos) a la troceadora.

Tal y como se ha explicado en “Sistemas de archivos raíz (/), QOpenSys y definidos por usuario” en la página 105, el sistema fuerza todas las autorizaciones sobre objeto, tanto si son visibles para la interfaz como si no. Por consiguiente, un usuario no puede trocear (suprimir) un objeto a menos que el usuario tenga la autorización *OBJEXIST para el objeto. Sin embargo, si su iSeries depende de la seguridad de acceso de menú en lugar de la seguridad de los objetos, el usuario del PC puede descubrir objetos del sistema de archivos QSYS.LIB disponibles para trocear.

A medida que vaya ampliando las utilizaciones del sistema y los diferentes métodos de acceso que puede proporcionar, irá descubriendo que la seguridad de acceso de menú no es suficiente. En el Capítulo 5, “Protección de la información con la autorización sobre objetos”, en la página 49 se tratan las estrategias para proporcionar el control de acceso de menú con la seguridad de objetos. Sin embargo, los servidores iSeries también proporcionan un modo sencillo para impedir el acceso al sistema de archivos QSYS.LIB a través de la estructura de directorios del sistema de archivos raíz. Puede utilizar la lista de autorizaciones de QPWFSERVER para controlar los usuarios que pueden acceder al sistema de archivos QSYS.LIB a través del directorio raíz.

Cuando la autorización de un usuario a la lista de autorizaciones QPWFSERVER es *EXCLUDE, el usuario no puede entrar en el directorio QSYS.LIB desde la estructura del directorio raíz. Si la autorización es *USE, el usuario puede entrar en el directorio. Cuando el usuario dispone de la autorización para entrar en el directorio, la autorización normal de objeto se aplica a todas las acciones que intente llevar a cabo en un objeto del sistema de archivos QSYS.LIB. En otras palabras, la autorización de la lista de autorizaciones QPWFSERVER actúa como una puerta al sistema de archivos QSYS.LIB completo. Para el usuario con la autorización *EXCLUDE, la puerta está bloqueada. Para el usuario con la autorización *USE (o cualquier autorización superior), la puerta está abierta.

En la mayor parte de las situaciones, los usuarios no necesitan utilizar una interfaz de directorio para acceder a los objetos del sistema de archivos QSYS.LIB. Probablemente, quizá desee establecer la autorización de uso público de la lista de autorizaciones QPWFSERVER para *EXCLUDE. Recuerde que la autorización de la lista de autorizaciones abre o cierra la puerta de todas las bibliotecas contenidas en el sistema de archivos QSYS.LIB, incluyendo las bibliotecas de usuario. Si algún usuario pone objeciones a esta exclusión, puede evaluar sus requisitos individualmente. Si lo considera necesario, puede autorizar explícitamente a un usuario individual a la lista de autorizaciones. Sin embargo, debe asegurarse de

que el usuario tenga la autorización adecuada para los objetos del sistema de archivos QSYS.LIB. De lo contrario, podrá suprimir objetos o bibliotecas enteras involuntariamente.

Notas:

1. Cuando se entrega el sistema, la autorización de uso público para la lista de autorizaciones QPWFSERVER es *USE.
2. Si autoriza a unusuario individual de forma explícita la lista de autorizaciones controla solamente el acceso al servidor de archivos de iSeries Access, el servidor de archivos de NetServer y el servicio de archivos entre los servidores iSeries. Ello no evitará el acceso a los mismos directorios desde FTP, ODBC u otras redes.

Protección de los directorios

Para acceder a un objeto del sistema de archivos raíz, debe leer la vía de acceso completa a dicho objeto. Para buscar un directorio, debe disponer de una autorización *X (*OBJOPR y *EXECUTE) para dicho directorio. Suponga, por ejemplo, que desea acceder al objeto siguiente:

```
/companya/customers/custfile.dat
```

Debe tener autorización *X para el directorio `companya` y para el directorio `customers`.

Con el sistema de archivos raíz, puede crear un enlace simbólico para un objeto. Un enlace simbólico es un seudónimo para el nombre de la vía de acceso. Generalmente, es más corto y más fácil de recordar que el nombre de la vía de acceso completa. Sin embargo, un enlace simbólico no crea una vía de acceso física diferente para el objeto. El usuario continúa necesitando la autorización *X para cada directorio y subdirectorio de la vía de acceso física al objeto.

Para los objetos del sistema de archivos raíz, puede utilizar la seguridad de directorios del mismo modo que utilizaría la seguridad de bibliotecas en el sistema de archivos QSYS.LIB. Por ejemplo, puede establecer la autorización de uso público de un directorio para *EXCLUDE e impedir así que los usuarios públicos puedan acceder a los objetos del árbol.

Seguridad para nuevos objetos

Al crear un objeto nuevo en el sistema de archivos raíz, la interfaz que utilice para crearlo determinará sus autorizaciones. Por ejemplo, si utiliza el mandato CRTDIR y sus valores por omisión, el nuevo directorio hereda todas las características de autorización de su directorio padre, incluidas las autorizaciones privadas, la autorización de grupo primario y la asociación de lista de autorizaciones. Los apartados siguientes describen cómo se determinan las autorizaciones para cada tipo de interfaz.

La autorización procede del directorio padre inmediato, no de los directorios superiores del árbol. Por consiguiente, como administrador de seguridad, necesita ver la autorización que asigna a los directorios de una jerarquía desde dos perspectivas:

- Cómo influye la autorización en el acceso a los objetos del árbol (por ejemplo, autorización de biblioteca).
- Cómo influye la autorización en los objetos que se acaban de crear (por ejemplo, el valor CRTAUT para bibliotecas).

Recomendación: Puede interesarle ofrecer a los usuarios que trabajen en el sistema de archivos integrado un directorio inicial (por ejemplo, /home/usrxxx) y luego establecer la seguridad de forma apropiada (por ejemplo como PUBLIC *EXCLUDE). Todos los directorios que cree el usuario bajo su directorio inicial, heredarán las autorizaciones.

A continuación se muestran algunas descripciones de la herencia de autorización para interfaces diferentes:

Utilización del mandato Crear directorio

Al crear un nuevo subdirectorio utilizando el mandato CRTDIR, existen dos opciones para especificar la autorización:

- Puede especificar la autorización de uso público (autorización sobre datos, autorización sobre objetos o ambas).
- Puede especificar *INDIR para la autorización sobre datos, la autorización sobre objetos o ambas. Al especificar *INDIR para la autorización sobre datos y la autorización sobre objetos, el sistema hace una copia exacta de toda la información sobre autorizaciones del directorio padre en el nuevo objeto, incluyendo la lista de autorizaciones, el grupo primario, la autorización de uso público y las autorizaciones privadas. (El sistema no copia la autorización privada que tiene el perfil QSYS o el perfil QSECOFR para el objeto).

Creación de un directorio con una API

Al crear un directorio utilizando la API mkdir(), especifica las autorizaciones sobre datos para el propietario y el grupo primario y el público (utilizando la correlación de autorización de *R, *W y *X). El sistema utiliza la información del directorio padre para establecer las autorizaciones sobre objetos para el propietario, el grupo primario y el público.

Puesto que los sistemas operativos de tipo UNIX no disponen del concepto de autorizaciones sobre objeto, la API mkdir() no ofrece soporte para especificar autorizaciones sobre objeto. Si desea autorizaciones sobre objeto diferentes, puede utilizar el mandato del servidor iSeries CHGAUT. Sin embargo, al eliminar algunas autorizaciones sobre objeto, la aplicación de tipo UNIX puede no funcionar como espera.

Creación de un archivo continuo con las API open() o creat()

Cuando utilice la API creat() para crear un archivo continuo, puede especificar las autorizaciones sobre datos para el propietario, el grupo primario y el público (utilizando las autorizaciones de tipo UNIX *R, *W y *X). El sistema utiliza la información del directorio padre para establecer las autorizaciones sobre objetos para el propietario, el grupo primario y el público.

También puede especificar estas autorizaciones al utilizar la API open() para crear un archivo continuo. Alternativamente, cuando utilice la API open() puede especificar que el objeto herede todas las autorizaciones del directorio padre. Esto se denomina `modalidad de herencia`. Al especificar la modalidad de herencia, el sistema crea una copia exacta para las autorizaciones padre, incluyendo la lista de autorizaciones, el grupo primario, la autorización pública y las autorizaciones privadas. Esta función es similar a especificar *INDIR en el mandato CRTDIR.

Creación de un objeto utilizando una interfaz de PC

Al utilizar una aplicación de PC para crear un objeto en el sistema de archivos raíz, el sistema hereda automáticamente todas las autorizaciones del directorio padre. Incluye la lista de autorizaciones, el grupo primario, la autorización de uso público y las autorizaciones privadas. Las aplicaciones de PC no equivalen en absoluto a especificar la autorización cuando se crea un objeto.

Sistema de archivos QFileSvr.400

Con el sistema de archivos QFileSvr.400, un usuario (USERX) de un sistema iSeries (SYSTEMA) puede acceder a los datos de otro sistema iSeries conectado (SYSTEMB).El USERX tiene una interfaz que es exactamente igual a la interfaz de Client Access. El servidor iSeries remoto (SYSTEMB) se muestra como un directorio con todos sus sistemas de archivos y subdirectorios.

Cuando USERX intenta acceder a SYSTEMB con esta interfaz, SYSTEMA envía el nombre de perfil de usuario USERX y la contraseña cifrada para SYSTEMB. El mismo perfil de usuario y la misma contraseña deben existir en SYSTEMB o SYSTEMB rechaza la petición.

Si SYSTEMB acepta la petición, USERX se muestra a SYSTEMB como cualquier otro usuario de Client Access. Las mismas normas de comprobación de autorización se aplican a todas las acciones que intente USERX.

Como administrador de seguridad, debe saber que el sistema de archivos QFileSvr.400 representa otra puerta posible al sistema. No puede asumir que está limitando a sus usuarios remotos a una conexión interactiva con paso a través de estación de pantalla. Si se está ejecutando el subsistema QSERVER y el sistema está conectado a otro sistema iSeries, los usuarios remotos pueden acceder al sistema como si estuvieran en un PC local ejecutando Client Access.Es más que probable que su sistema disponga de una conexión que precise que se ejecute el subsistema QSERVER. Este sería otro de los motivos por los que un esquema de autorización sobre objeto resulta esencial.

Sistema de archivos de red

El sistema de archivos de red (NFS) proporciona acceso a sistemas con implementaciones NFS. NFS es un método estándar del mercado para compartir información entre usuarios de los sistemas de la red. La mayor parte de los sistemas operativos importantes (incluyendo sistemas operativos de PC) proporciona NFS. Para sistemas UNIX, NFS es el método principal para acceder a los datos. Los servidores iSeries pueden actuar como un cliente NFS o como un servidor NFS.

Si es un administrador de seguridad de un sistema iSeries que actúa como un servidor NFS, necesita comprender y gestionar los aspectos de seguridad de NFS. A continuación se presentan algunas sugerencias y consideraciones:

- Debe iniciar explícitamente la función de servidor NFS utilizando el mandato STRNFSSVR. Controle quién está autorizado a utilizar este mandato.
- Para que un directorio o un objeto estén disponibles para los clientes NFS debe `exportarlos`. Por consiguiente, dispone de un control específico a través del cual parte de su sistema estará disponible a los clientes NFS de la red.
- Al exportar, puede especificar los clientes que deben disponer de acceso a los objetos. La identificación de un cliente se lleva a cabo mediante el nombre del

sistema o la dirección IP. Un cliente puede ser un PC individual o un servidor iSeries o un sistema UNIX completo. En terminología NFS, el cliente (dirección IP) se denomina una `máquina`.

- Al exportar, puede especificar el acceso de sólo lectura o de lectura/grabación para cada máquina que tenga acceso a un directorio u objeto exportado. En la mayoría de los casos, quizá desee proporcionar acceso de sólo lectura.
- El NFS no proporciona protección de contraseña. Su diseño y finalidad es compartir datos entre una comunidad de sistemas autorizados. Cuando un usuario solicita acceso, el servidor recibe el `uid` del usuario. A continuación se incluyen algunas consideraciones acerca del `uid`:
  - El servidor iSeries intenta localizar un perfil de usuario con el mismo `uid`. Si encuentra un `uid` que coincide, utiliza las credenciales del perfil de usuario. Las credenciales son un término NFS para describir la utilización de la autorización de un usuario. Es similar al intercambio de perfiles de otras aplicaciones de servidor iSeries.
  - Al exportar un directorio u objeto, puede especificar si se permitirá el acceso mediante un perfil con autorización raíz. El servidor NFS de los servidores iSeries compara la autorización raíz con la autorización especial de *ALLOBJ. Si especifica que no permitirá la autorización raíz, un usuario NFS con un `uid` que se correlacione con un perfil de usuario con autorización especial *ALLOBJ no podrá acceder al objeto que tenga ese perfil. En su lugar, si se permite el acceso anónimo, el peticionario se correlacionará con el perfil anónimo.
  - Al exportar un directorio u objeto, puede especificar si se permitirán peticiones anónimas. Una petición anónima es una petición con un `uid` que no coincide con ningún `uid` del sistema. Si elige permitir peticiones anónimas, el sistema correlaciona el usuario anónimo con el perfil de usuario QNFSANON suministrado por IBM. Este perfil de usuario no dispone de ninguna autorización especial o explícita. (Si lo desea, en la exportación, puede especificar un perfil de usuario diferente para las peticiones anónimas).
- Cuando el servidor iSeries participa en una red NFS (o en cualquier red con sistemas UNIX que dependan de los `uid`), probablemente necesite gestionar sus propios `uid` en lugar de permitir que el sistema los asigne automáticamente. Debe coordinar los `uid` con otros sistemas de la red.

  Quizá se dé cuenta de que debe cambiar los `uid` (incluso para perfiles de usuario suministrados por IBM) para disponer de compatibilidad con otros sistemas de la red. Existe un programa disponible para simplificar el cambio de `uid` para un perfil de usuario. (Al cambiar el `uid` para un perfil de usuario, también debe cambiar el `uid` de todos los objetos que pertenecen al perfil, tanto en el directorio raíz como en el directorio QOpenSrv.) El programa QSYCHGID cambia automáticamente el `uid` tanto en el perfil de usuario como en los objetos pertenecientes al mismo. Para obtener información sobre cómo utilizar este programa, consulte el manual *iSeries System API Reference*.

Capítulo 12. Protección de las comunicaciones APPC

Cuando el sistema forma parte de una red conjuntamente con otros sistemas, es como si se abrieran nuevas puertas para acceder a él. Como administrador de seguridad, debe tener presentes las opciones que puede utilizar para controlar la entrada en el sistema en un entorno APPC.

Las comunicaciones avanzadas programa a programa (APPC) son una forma de comunicación entre los sistemas, incluidos los PC. El paso a través de estación de pantalla, la gestión de datos distribuidos e iSeries Access para Windows pueden utilizar las comunicaciones APPC.

Los temas que se tratan a continuación proporcionan información básica acerca de cómo funcionan las comunicaciones APPC y cómo se puede establecer la seguridad idónea. Estos temas se concentran principalmente en los elementos relativos a la seguridad de una configuración APPC. Para adaptar este ejemplo a su caso, tendrá que trabajar conjuntamente con quienes gestionan la red de comunicaciones y quizás también con los proveedores de aplicaciones. Utilice esta información como punto de partida para comprender las cuestiones de seguridad y las opciones disponibles para APPC.

La seguridad nunca es gratuita. Algunas sugerencias para facilitar la seguridad de la red pueden convertir la administración de la red en una tarea más compleja. Por ejemplo, esta publicación no hace hincapié en APPN (Redes avanzadas de igual a igual), ya que la seguridad es más fácil de comprender y gestionar sin APPN. Sin embargo, sin APPN, el administrador de la red debe crear manualmente la información de configuración que APPN crea de forma automática.

Los PC también usan comunicaciones

Una gran cantidad de métodos para conectar los PC a los servidores iSeries dependen de las comunicaciones, como APPC o TCP/IP. Cuando lea los temas siguientes, asegúrese de que tiene en cuenta las cuestiones de seguridad de la conexión a otros sistemas y a los PC. Cuando diseñe la protección de la red, asegúrese de que no afecta negativamente a los PC que están conectados al sistema.

Terminología de APPC

APPC proporciona la posibilidad de que un usuario de un sistema trabaje en otro sistema. El sistema desde el que se inicia la petición recibe uno de estos nombres:

- **Sistema (de) origen**
- **Sistema local**
- **Cliente**

El sistema que recibe la petición se denomina:

- **Sistema (de) destino**
- **Sistema remoto**
- **Servidor**

Elementos básicos de las comunicaciones APPC

Desde el punto de vista del administrador de seguridad, deben darse las condiciones que se indican a continuación para que un usuario de un sistema (SISTEMA1) pueda trabajar en otro sistema (SISTEMA2):

- El sistema origen (SISTEMA1) debe proporcionar una vía de acceso al sistema destino (SISTEMA2). Esta vía recibe el nombre de **sesión APPC**.
- El sistema destino debe identificar al usuario y asociarlo con un perfil de usuario.El sistema destino debe soportar el algoritmo de cifrado del sistema origen (consulte "Niveles de contraseña" en la página 16 para obtener más información).
- El sistema destino debe iniciar un trabajo para el usuario con el entorno adecuado (valores de gestión de trabajo).

En los temas siguientes se tratan estos elementos y de qué manera están relacionados con la seguridad. El administrador de seguridad del sistema destino tiene la responsabilidad principal de garantizar que los usuarios de APPC no violan la seguridad. Sin embargo, si los administradores de seguridad de ambos sistemas trabajan conjuntamente, la gestión de la seguridad de APPC es una tarea mucho más sencilla.

Ejemplo: Una sesión APPC básica

En un entorno APPC, cuando un usuario o una aplicación de un sistema solicita acceso a otro sistema, ambos sistemas establecen una sesión. Para establecer la sesión, los sistemas deben enlazar dos descripciones de dispositivo APPC coincidentes. El parámetro de nombre de ubicación remota (RMTLOCNAME) de la descripción de dispositivo del SISTEMA1 debe coincidir con el parámetro de ubicación local (LCLLOCNAME) de la descripción de dispositivo del SISTEMA2 y viceversa.

Para que dos sistemas establezcan una sesión APPC, las contraseñas de ubicación de las descripciones de dispositivo APPC en SISTEMA1 y SISTEMA2 deben ser idénticas. En ambas debe especificarse *NONE o un mismo valor.

Si las contraseñas tienen un valor distinto de *NONE, se almacenan y se transmiten en formato cifrado. Si coinciden, los sistemas establecen una sesión. Si no coinciden, la petición del usuario se rechaza. La especificación de contraseñas de ubicación en los sistemas recibe el nombre de **enlace protegido**.

Nota: No todos los sistemas proporcionan soporte para la función de enlace protegido.

Restricción de las sesiones APPC

Como administrador de seguridad de un sistema origen, puede utilizar la autorización sobre objeto para controlar quién intenta acceder a otros sistemas. Establezca la autorización de uso público para las descripciones de dispositivo APPC en *EXCLUDE y otorgue autorización *CHANGE a usuarios determinados. Utilice el valor del sistema QLMTSECOFR para impedir que los usuarios que tengan autorización especial *ALLOBJ utilicen las comunicaciones APPC.

Como administrador de seguridad de un sistema destino, también debe utilizar la autorización sobre los dispositivos APPC para impedir que los usuarios inicien una sesión APPC en su sistema. Sin embargo, debe saber qué ID de usuario intentará acceder a la descripción de dispositivo APPC. En el apartado "Cómo un usuario de

APPC obtiene acceso al sistema destino" se describe cómo los servidores iSeries asocian un ID de usuario con una petición de sesión APPC.

Nota: Puede utilizar el mandato Imprimir objetos con autorización de uso público (PRTPUBAUT *DEVD) y el mandato Imprimir autorizaciones privadas (PRTPVTAUT *DEVD) para averiguar quién posee autorización sobre las descripciones de dispositivo de su sistema.

Cuando su sistema utiliza APPN, crea automáticamente un dispositivo APPC nuevo si no hay ningún dispositivo disponible para la ruta elegida por el sistema. Un método para restringir el acceso a los dispositivos APPC de un sistema que utiliza APPN es crear una lista de autorizaciones. La lista de autorizaciones contiene la lista de los usuarios que deben tener autorización para los dispositivos APPC. Utilice el mandato Cambiar valor por omisión de mandato (CHGCMDDFT) para cambiar el mandato CRTDEVAPPC. Para el parámetro de autorización (AUT) del mandato CRTDEVAPPC, establezca el valor por omisión para la lista de autorizaciones que ha creado.

Nota: Si el sistema utiliza un idioma que no es el inglés, debe cambiar el valor por omisión del mandato en la biblioteca QSYSxxxx para cada idioma nacional que se utilice en el sistema.

Utilice el parámetro de contraseña de ubicación (LOCPWD) en la descripción de dispositivo APPC para validar la identidad de otro sistema que está solicitando una sesión en su sistema (para un usuario o una aplicación). La contraseña de ubicación puede ayudarle a detectar un sistema impostor.

Cuando utilice contraseñas de ubicación, debe trabajar en coordinación con los administradores de seguridad de los demás sistemas de la red. También debe controlar quién puede crear o cambiar las descripciones de dispositivo APPC y las listas de configuraciones. El sistema requiere la autorización especial *IOSYSCFG para utilizar los mandatos que trabajan con listas de configuraciones y dispositivos APPC.

Nota: Cuando utiliza APPN, las contraseñas de ubicación se almacenan en la lista de configuración QAPPNRMT en lugar de en las descripciones de dispositivo.

Cómo un usuario de APPC obtiene acceso al sistema destino

Cuando los sistemas establecen la sesión APPC, crean una vía de acceso para que el usuario solicitante llegue a la "puerta" del sistema destino. Algunos otros elementos determinan lo que debe hacer el usuario para conseguir la entrada al otro sistema.

En los temas siguientes se describen los elementos que determinan cómo un usuario de APPC obtiene el acceso a un sistema destino.

Métodos del sistema para enviar información sobre un usuario

La arquitectura APPC proporciona tres métodos para enviar información de seguridad acerca de un usuario desde el sistema origen al sistema destino. Estos métodos reciben el nombre de **valores de seguridad con arquitectura**. En la Tabla 18 en la página 118 se muestran estos métodos:

Nota: La publicación *APPC Programming* proporciona más información acerca de los valores de seguridad con arquitectura.

Tabla 18. Valores de seguridad en la arquitectura APPC

Valor de seguridad de arquitectura	ID de usuario enviado al sistema destino	Contraseña enviada al sistema destino
NONE	No	No
SAME	Sí[1]	Vea la nota 2.
Programa	Sí	Yes[3]

Notas:

1. El sistema origen envía el ID de usuario si el sistema destino tiene el valor SECURELOC(*YES) o SECURELOC(*VFYENCPWD).
2. El usuario no entra una contraseña en la petición porque el sistema origen ya ha verificado la contraseña. En el caso de SECURELOC(*YES) y de SECURELOC(*NO), el sistema origen no envía la contraseña. En el caso de SECURELOC(*VFYENCPWD), el sistema de origen recupera la contraseña cifrada almacenada y la envía (en formato cifrado).
3. El sistema envía las contraseñas cifradas si el sistema origen y el sistema destino ofrecen soporte para el cifrado de contraseñas. De lo contrario, la contraseña no se cifra.

La aplicación que el usuario solicita determina el valor de seguridad con arquitectura. Por ejemplo, SNADS siempre utiliza SECURITY(NONE). DDM utiliza SECURITY(SAME). Con el paso a través de estación de pantalla, el usuario especifica el valor de seguridad utilizando parámetros del mandato STRPASTHR.

En todos los casos, el sistema destino decide si se acepta una petición con el valor de seguridad que está especificado en el sistema origen. En algunos casos, el sistema destino puede rechazar totalmente la petición. En otros casos, el sistema destino puede forzar la utilización de otro valor de seguridad. Por ejemplo, cuando un usuario especifica un ID de usuario y una contraseña en el mandato STRPASTHR, la petición utiliza SECURITY(PGM). Sin embargo, si el valor del sistema QRMTSIGN es *FRCSIGNON en el sistema destino, el usuario sigue visualizando la pantalla Inicio de sesión. Con el valor *FRCSIGNON, el sistema siempre utiliza SECURITY(NONE), que es lo mismo que no entrar ID de usuario ni contraseña en el mandato STRPASTHR.

Notas:

1. Los sistemas de origen y de destino negocian el valor de seguridad antes de enviar datos. En el caso en que el sistema destino especifique SECURELOC(*NO) y la petición sea SECURITY(SAME), por ejemplo, el sistema destino indicará al sistema origen que se utilizará SECURITY(NONE). El sistema origen no envía el ID de usuario.
2. El sistema destino rechaza una petición de sesión una vez que ha caducado la contraseña del usuario en el sistema destino. Esto sólo es aplicable a las peticiones de conexión que envían una contraseña, lo que incluye lo siguiente:
   - Peticiones de sesión del tipo SECURITY(PROGRAM).
   - Peticiones de sesión del tipo SECURITY(SAME) cuando el valor de SECURELOC es *VFYENCPWD.

Opciones para repartir la responsabilidad de la seguridad de la red

Cuando su sistema participa en una red, debe decidir si confiará en los otros sistemas para la validación de la identidad de un usuario que intente entrar en su

sistema. ¿Confiará en el SISTEMA1 para asegurarse de que USUARIO1 es realmente USUARIO1 (o de que QSECOFR es, en efecto, QSECOFR)? ¿O exigirá que el usuario proporcione de nuevo el ID de usuario y la contraseña?

El parámetro de proteger ubicación (SECURELOC) de la descripción de dispositivo APPC en el sistema destino indica si el sistema origen es una ubicación protegida (en la que se confiará).

Cuando ambos sistemas están ejecutando un release que soporta *VFYENCPWD, SECURELOC(*VFYENCPWD) proporciona protección adicional cuando las aplicaciones utilizan SECURITY(SAME). Aunque el solicitante no entre una contraseña en la petición, el sistema origen recupera la contraseña del usuario y la envía con la petición. Para que ésta sea satisfactoria, el usuario debe tener el mismo ID de usuario y la misma contraseña en ambos sistemas.

Cuando el sistema destino especifica SECURELOC(*VFYENCPWD) y el sistema origen no da soporte a este valor, el sistema destino manejará la petición como SECURITY(NONE).

En la Tabla 19 se ilustra el funcionamiento conjunto del valor de seguridad con arquitectura y el valor SECURELOC:

Tabla 19. Funcionamiento conjunto del valor de seguridad de APPC y del valor SECURELOC

Sistema origen	**Sistema destino**	
Valor de seguridad de arquitectura	**Valor SECURELOC**	**Perfil de usuario para el trabajo**
NONE	Cualquiera	Usuario por omisión[1]
SAME	*NO	Usuario por omisión[1]
	*YES	El mismo nombre de perfil de usuario del solicitante en el sistema origen
	*VFYENCPWD	El mismo nombre de perfil de usuario del solicitante del sistema origen. El usuario debe tener de la misma contraseña en ambos sistemas.
Programa	Cualquiera	Los perfiles de usuario que se han especificado en la solicitud del sistema origen.

Notas:

1. El usuario por omisión lo determina la entrada de comunicaciones de la descripción de subsistema. Se describe en "Asignación de perfiles de usuario para trabajos en el sistema destino".

Asignación de perfiles de usuario para trabajos en el sistema destino

Cuando un usuario solicita un trabajo APPC que está en otro sistema, la petición tiene un nombre de modalidad asociado. Dicho nombre puede provenir de la petición del usuario o puede ser un valor por omisión de los atributos de red del sistema origen.

El sistema destino utiliza el nombre de modalidad y el nombre de dispositivo APPC para determinar cómo se ejecutará el trabajo. El sistema destino busca en los

subsistemas activos una entrada de comunicaciones que sea la más adecuada para el nombre de dispositivo APPC y el nombre de modalidad.

La entrada de comunicaciones especifica el perfil de usuario que el sistema utilizará para las peticiones SECURITY(NONE). A continuación se facilita un ejemplo de una entrada de comunicaciones en una descripción de subsistema.

```
                        Visualizar entradas de comunicaciones

Descripción subsistema:  QCMN           Estado:   ACTIVO

                          Descripción                  Usuario        Máx
Dispositivo   Modalidad   de trabajo     Biblioteca    omisión       activos
*ALL          *ANY        *USRPRF                      *SYS          *NOMAX
*ALL          QPCSUPP     *USRPRF                      *NONE         *NOMAX
```

En la Tabla 20 se muestran los valores posibles para el parámetro de usuario por omisión en una entrada de comunicaciones:

Tabla 20. Valores posibles para el parámetro de usuario por omisión

Valor	Resultado
***NONE**	No hay ningún usuario por omisión disponible. Si el sistema origen no proporciona un ID de usuario en la petición, el trabajo no se ejecutará.
***SYS**	Solamente se ejecutarán los programas proporcionados por IBM. No se ejecutará ninguna aplicación de usuario.
nombre de usuario	Si el sistema origen no envía un ID de usuario, el trabajo se ejecuta bajo este perfil de usuario.

Puede utilizar el mandato Imprimir descripción de subsistema (PRTSBSDAUT) para imprimir la lista de todos los subsistemas que tengan entradas de comunicaciones con un perfil de usuario por omisión.

Opciones de paso a través de estación de pantalla

El paso a través de estación de pantalla es un ejemplo de aplicación que utiliza comunicaciones APPC. Puede utilizar el paso a través de estación de pantalla para iniciar la sesión en otro sistema que esté conectado al suyo a través de una red.

La Tabla 21 en la página 121 muestra ejemplos de peticiones de paso a través (mandato STRPASTHR) y cómo las maneja el sistema destino. Para el paso a través de estación de pantalla, el sistema utiliza los elementos básicos de las comunicaciones APPC y el valor del sistema de inicio de sesión remoto (QRMTSIGN).

Nota: Las peticiones de paso a través de estación de pantalla ya no se direccionan a través de los subsistemas QCMN o QBASE. A partir de la V4R1, se direccionan a través del subsistema QSYSWRK. Antes de la V4R1 se presuponía que, al no haber iniciado los subsistemas QCMD o QBASE, el paso a través de estación de pantalla no funcionaría. Esto ya no es verdad. Puede forzar el paso a través de estación de pantalla para que vaya a través de QCMN (o QBASE, si está activo) estableciendo el valor del sistema QPASTHRSVR en 0.

Tabla 21. Ejemplos de peticiones de inicio de sesión de paso a través

Valores del mandato STRPASTHR		**Sistema destino**		
ID de usuario	**Contraseña**	**Valor SECURELOC**	**Valor QRMTSIGN**	**resultado**
*NONE	*NONE	Cualquiera	Cualquiera	El usuario debe iniciar la sesión en el sistema de destino.
Nombre de perfil de usuario	No entrada	Cualquiera	Cualquiera	La petición falla.
*CURRENT	No entrada	*NO	Cualquiera	La petición falla.
		*YES	*SAMEPRF	Un trabajo interactivo se inicia con el mismo nombre de perfil de usuario que el perfil de usuario del sistema origen. No se pasa ninguna contraseña al sistema remoto. El nombre de perfil de usuario debe existir en el sistema de destino.
			*VERIFY	
			*FRCSIGNON	El usuario debe iniciar la sesión en el sistema de destino.
		*VFYENCPWD	*SAMEPRF	Un trabajo interactivo se inicia con el mismo nombre de perfil de usuario que el perfil de usuario del sistema origen. El sistema de origen recupera la contraseña del usuario y la envía al sistema remoto. El nombre de perfil de usuario debe existir en el sistema de destino.
			*VERIFY	
			*FRCSIGNON	El usuario debe iniciar la sesión en el sistema de destino.
*CURRENT (o el nombre del perfil de usuario actual para el trabajo)	Entrada	Cualquiera	*SAMEPRF	Un trabajo interactivo se inicia con el mismo nombre de perfil de usuario que el perfil de usuario del sistema origen. La contraseña *se envía* al sistema remoto. El nombre de perfil de usuario debe existir en el sistema de destino.
			*VERIFY	
			*FRCSIGNON	El usuario debe iniciar la sesión en el sistema de destino.

Tabla 21. Ejemplos de peticiones de inicio de sesión de paso a través (continuación)

Valores del mandato STRPASTHR		Sistema destino		
ID de usuario	**Contraseña**	**Valor SECURELOC**	**Valor QRMTSIGN**	**resultado**
Nombre de perfil de usuario (distinto del nombre de perfil de usuario actual para el trabajo)	Entrada	Cualquiera	*SAMEPRF	La petición falla.
			*VERIFY	Un trabajo interactivo se inicia con el mismo nombre de perfil de usuario que el perfil de usuario del sistema origen. La contraseña *se envía* al sistema remoto. El nombre de perfil de usuario debe existir en el sistema de destino.
			*FRCSIGNON	Un trabajo interactivo se inicia con el nombre especificado de perfil de usuario. La contraseña se envía al sistema destino. El nombre de perfil de usuario debe existir en el sistema destino.

Cómo evitar asignaciones de dispositivos inesperadas

Cuando se produce una anomalía en un dispositivo activo, el sistema intenta su recuperación. Bajo ciertas circunstancias, cuando la conexión se interrumpe otro usuario puede restablecer accidentalmente la sesión que ha sufrido la anomalía. Por ejemplo, suponga que el USUARIO1 ha apagado una estación de trabajo sin finalizar la sesión. El USUARIO2 podría encender la estación de trabajo y reiniciar la sesión del USUARIO1 sin conectarse.

Para evitar esta posibilidad, establezca el valor del sistema de Acción de error de E/S de dispositivo (QDEVRCYACN) en *DSCMSG. Cuando se produce una anomalía en un dispositivo, el sistema finalizará el trabajo del usuario.

Control de mandatos remotos y trabajos de proceso por lotes

Hay varias opciones disponibles para ayudarle a controlar qué trabajos y mandatos remotos se pueden ejecutar en el sistema, incluidos los siguientes:

- Si su sistema utiliza DDM, puede limitar el acceso a los archivos DDM para impedir que los usuarios utilicen el mandato Someter mandato remoto (SBMRMTCMD) desde otro sistema. Para utilizar el mandato SBMRMTCMD, el usuario debe poder abrir un archivo DDM. También es necesario restringir la capacidad de crear archivos DDM.
- Puede especificar un programa de salida para el valor del sistema Acceso a petición DDM (DDMACC). En el programa de salida puede evaluar todas las peticiones DDM antes de permitirlas.
- Puede utilizar el atributo de red Acción de trabajo de red (JOBACN) para impedir que se sometan trabajos de red o que se ejecuten automáticamente.
- Puede especificar explícitamente qué peticiones de programa se pueden ejecutar en un entorno de comunicaciones eliminando la entrada de direccionamiento PGMEVOKE de las descripciones de subsistemas. La entrada de direccionamiento PGMEVOKE permite al solicitante especificar el programa que

se ejecuta. Cuando se elimina esta entrada de direccionamiento de las descripciones de subsistemas (por ejemplo, de la descripción del subsistema QCMN), debe añadir entradas de direccionamiento para las peticiones de comunicaciones que deben ejecutarse satisfactoriamente.

En la "Peticiones de TPN con arquitectura" en la página 97 se enumeran los nombres de programas para las peticiones de comunicaciones emitidas por las aplicaciones proporcionadas por IBM.Para cada petición que desee permitir, puede añadir una entrada de direccionamiento con el valor de comparación y el nombre de programa iguales a los del nombre de programa.

Cuando se utiliza este método es necesario saber cuál es el entorno de gestión de trabajo del sistema y los tipos de peticiones de comunicaciones que se producen en el sistema. Si es posible, deben comprobarse todos los tipos de peticiones de comunicaciones para asegurarse de que funcionan correctamente después de cambiar las entradas de direccionamiento. Cuando una petición de comunicaciones no encuentra una entrada de direccionamiento disponible, se recibe el mensaje CPF1269. Otra alternativa (con menos posibilidad de error, pero menos efectiva) es establecer la autorización de uso público para *EXCLUDE para los programas de transacción que no desea ejecutar en el sistema.

Nota: En la publicación *Work Management* puede obtener más información acerca de las entradas de direccionamiento y de cómo maneja el sistema las peticiones de arranque de programa.

Evaluación de la configuración de APPC

Puede utilizar el mandato Imprimir seguridad de comunicaciones (PRTCMNSEC) o bien opciones de menú para imprimir los valores relativos a la seguridad de la configuración APPC. En los temas que figuran a continuación se describe la información de los informes.

Parámetros relevantes para los dispositivos APPC

En la Figura 9 se muestra un ejemplo del informe de las comunicaciones correspondiente a las descripciones de dispositivos. La Figura 10 en la página 124 contiene un ejemplo del informe correspondiente a las listas de configuraciones. Después de los informes encontrará explicaciones de los campos de los informes.

```
                          Información de comunicaciones (informe completo)
                                                                                                SYSTEM4
 Tipo de objeto . . . . . :   *DEVD

                                                                                    Sesión      Arranque
Nombre          Tipo          Categoría     Ubicación    Contraseña   Posibil.    Una sola    preesta-    programa
objeto          objeto        dispositivo   protegida    ubicación    APPN        sesión      blecida     SNUF

 CDMDEV1         *DEVD         *APPC           *NO          *NO         *NO         *YES        *NO
 CDMDEV2         *DEVD         *APPC           *NO          *NO         *NO         *YES        *NO
```

Figura 9. Descripciones de dispositivo APPC-Informe de ejemplo

```
                  Visualizar lista de configuraciones          Página   1
                              SYSTEM4  12/17/95  07:24:36
Lista de configuraciones . . . . . :   QAPPNRMT
 Tipo de lista de configuraciones . :   *APPNRMT
 Texto  . . . . . . . . . . . . . . :
 ----------------Ubicaciones remotas APPN----------------
           ID de               Punto     ID red
 Ubicac.   red       Ubicac.   control   punto     Ubicac.
 remota    remoto    local     remoto    control   protegida
 SYSTEM36  APPN      SYSTEM4   SYSTEM36  APPN       *NO
 SYSTEM32  APPN      SYSTEM4   SYSTEM32  APPN       *NO
 SYSTEMU   APPN      SYSTEM4   SYSTEM33  APPN       *YES
 SYSTEMJ   APPN      SYSTEM4   SYSTEMJ   APPN       *NO
 SYSTEMR2  APPN      SYSTEM4   SYSTEM1   APPN       *NO
 ------------------------Ubicaciones remotas APPN--------------------------
           ID de                                          Punto     Sesión
 Ubicac.   red       Ubicac.   Una sola   Número de    control    preesta-
 remota    remoto    local     sesión   conversaciones  local     blecida
 SYSTEM36  APPN      SYSTEM4    *NO             10      *NO        *NO
 SYSTEM32  APPN      SYSTEM4    *NO             10      *NO        *NO
```

Figura 10. Informe de lista de configuraciones-Ejemplo

Campo Ubicación protegida

El campo Ubicación protegida (SECURELOC) especifica si el sistema local confía en el sistema remoto para que éste último efectúe la verificación de las contraseñas en lugar del sistema local. El campo SECURELOC solamente incumbe a las aplicaciones que utilizan el valor SECURITY(SAME), como las aplicaciones DDM y las aplicaciones que utilizan la API de comunicaciones CPI.

SECURELOC(*YES) hace que el sistema local sea vulnerable a posibles deficiencias en el sistema remoto. Todos los usuarios que existan en ambos sistemas pueden llamar a programas del sistema local. Esto es especialmente peligroso, ya que el perfil de usuario QSECOFR (responsable de seguridad) existe en todos los sistemas iSeries y posee la autorización especial *ALLOBJ.Si un sistema de la red no protege correctamente la contraseña de QSECOFR, otros sistemas que traten a éste como ubicación protegida corren riesgos.

Si se utiliza SECURELOC(*VFYENCPWD), el sistema es menos vulnerable a otros sistemas que no protegen sus contraseñas adecuadamente. Un usuario que solicite una aplicación que utilice SECURITY(SAME) debe tener el mismo ID de usuario y la misma contraseña en ambos sistemas. SECURELOC(*VFYENCPWD) requiere la utilización de métodos de administración de contraseñas en la red para que los usuarios tengan la misma contraseña en todos los sistemas.

Nota: Sólo se ofrece soporte para SECURELOC(*VFYENCPWD) entre sistemas que ejecuten la V3R2, la V3R7 o la V4R1. Si el sistema de destino especifica SECURELOC(*VFYENCPWD) y el sistema de origen no da soporte a esta función, la petición se trata como SECURITY(NONE).

Si un sistema especifica SECURELOC(*NO), las aplicaciones que utilicen SECURITY(SAME) necesitarán un usuario por omisión para ejecutar programas. El usuario por omisión depende de la descripción de dispositivo y de la modalidad asociadas con la petición. (Consulte el apartado “Asignación de perfiles de usuario para trabajos en el sistema destino” en la página 119.)

Campo Contraseña de ubicación

El campo Contraseña de ubicación determina si dos sistemas intercambiarán contraseñas para verificar que el sistema solicitante no es un sistema impostor. En el apartado “Ejemplo: Una sesión APPC básica” en la página 116 se facilita más información acerca de las contraseñas de ubicación.

Campo Posibilidad de APPN

El campo Posibilidad de APPN (APPN) especifica si el sistema remoto puede dar soporte a las funciones de red avanzada o si está limitado a las conexiones de un solo salto. APPN(*YES) significa lo siguiente:

- Si el sistema remoto es un nodo de la red, puede conectar el sistema local a otros sistemas. Esta posibilidad recibe el nombre de **direccionamiento de nodo intermedio**. Significa que los usuarios de su sistema pueden utilizar el sistema remoto como ruta a una red más amplia.
- Si el sistema local es un nodo de red, el sistema remoto puede utilizar el sistema local para conectarse a otros sistemas. Los usuarios del sistema remoto pueden utilizar su sistema como ruta a una red más amplia.

  Nota: Puede utilizar el mandato DSPNETA para determinar si un sistema es un nodo de red o un nodo final.

Campo Una sola sesión

El campo Una sola sesión (SNGSSN) indica si el sistema remoto puede ejecutar más de una sesión al mismo tiempo utilizando la misma descripción de dispositivo APPC. SNGSSN(*NO) suele utilizarse porque elimina la necesidad de crear varias descripciones de dispositivo para un sistema remoto. Por ejemplo, los usuarios de PC a menudo desean más de una sesión de emulación 5250 y sesiones para las funciones de servidor de archivos y servidor de impresión. Con SNGSSN(*NO), puede proporcionar esta función con una descripción de dispositivo para el PC en el sistema iSeries.

SNGSSN(*NO) significa que debe confiar en los procedimientos operativos de seguridad de los usuarios de PC y de otros usuarios APPC. Su sistema es vulnerable por un usuario del sistema remoto que inicie una sesión no autorizada que utiliza la misma descripción de dispositivo que una sesión existente. (A esta práctica se le denomina en algunos casos **parasitismo**.)

Campo Sesión preestablecida

El campo Sesión preestablecida (PREESTSSN) para un dispositivo de una sola sesión controla si el sistema local inicia una sesión con el sistema remoto cuando este se pone en contacto por primera vez con el sistema local. PREESTSSN(*NO) significa que el sistema local espera a iniciar una sesión a que una aplicación solicite una sesión con el sistema. PREESTSSN(*YES) es útil para minimizar el tiempo que tarda un programa de aplicación en completar la conexión.

PREESTSSN(*YES) impide que el sistema se desconecte de una línea conmutada (de marcación) que ya no se utiliza. La aplicación o el usuario deben desactivar explícitamente la línea. PREESTSSN(*YES) puede aumentar el tiempo que el sistema local es vulnerable al parasitismo en la sesión.

Campo Arranque de programa SNUF

El campo Arranque de programa SNUF indica si el sistema remoto puede arrancar programas del sistema local. *YES significa que el esquema de autorización sobre objetos del sistema local debe ser apropiado para proteger objetos cuando los usuarios del sistema remoto arrancan trabajos y ejecutan programas en el sistema local.

Parámetros para los controladores APPC

La Figura 11 muestra un ejemplo del informe de las comunicaciones correspondiente a las descripciones de controlador. Después del informe encontrará explicaciones de los campos del informe.

```
                    Información de comunicaciones (informe completo)
                                                                                SYSTEM4
Tipo de objeto . . . . . :   *CTLD

Nombre    Tipo      Categoría    Creación  Controlad.   Direcc.    Posibil.  Sesiones   Temporiz.    Segundos  Nombre
objeto    objeto    controlad.    autom.   conmutado    llamada     APPN        CP      desconex.     supres.  dispos.
CTL01     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES           0        1440    AARON
CTL02     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES           0        1440    BASIC
CTL03     *CTLD     *APPC         *YES       *YES        *DIAL      *YES       *YES           0        1440    *NONE
```

Figura 11. Descripciones de controlador APPC-Ejemplo de informe

Campo Creación automática

En una descripción de línea, el campo Creación automática (AUTOCRTCTL) indica si el sistema local creará automáticamente una descripción de controlador cuando una petición de entrada no encuentre una descripción de controlador coincidente. En una descripción de controlador, el campo Creación automática (AUTOCRTDEV) especifica si el sistema local creará automáticamente una descripción de dispositivo cuando una petición de entrada no encuentre una descripción de dispositivo coincidente.

En el caso de los controladores con posibilidades de APPN, este campo no tiene efecto alguno. El sistema crea automáticamente descripciones de dispositivo cuando es necesario, independientemente de cómo haya definido el campo de creación automática.

Cuando se especifica *YES para una descripción de línea, cualquier persona con acceso a la línea puede conectarse al sistema. Ello incluye ubicaciones que están conectadas mediante puentes y direccionadores.

Campo Sesiones de punto de control

En los controladores con posibilidad de APPN, el campo Sesiones de punto de control (CPSSN) controla si el sistema establecerá automáticamente una conexión APPC con el sistema remoto. El sistema utiliza la sesión CP para intercambiar información y estado de red con el sistema remoto. El intercambio de información actualizada entre nodos de red APPN es especialmente importante para que la red funcione correctamente.

Cuando se especifica *YES, las líneas conmutadas desocupadas no se desconectan automáticamente. Esto hace que su sistema sea más vulnerable a que haya una sesión parásito.

Campo Temporizador de desconexión

Para un controlador APPC, el campo Temporizador de desconexión indica cuánto tiempo debe transcurrir sin que se utilice un controlador (sin sesiones activas) antes de que el sistema desconecte la línea con el sistema remoto. Este campo tiene dos valores. El primer valor indica cuánto tiempo permanecerá activo el controlador desde el momento en que se contacta con él inicialmente. El segundo valor determina cuánto tiempo espera el sistema tras la finalización de la última sesión en el controlador antes de desconectar la línea.

El sistema utiliza el temporizador de desconexión solamente cuando el valor del campo de desconexión conmutada (SWTDSC) es *YES.

Si aumenta estos valores, el sistema será más vulnerable a las sesiones parásito.

Parámetros para las descripciones de línea

En la Figura 12 se muestra un ejemplo del informe de las comunicaciones correspondiente a las descripciones de línea. Después del informe encontrará explicaciones de los campos del informe.

```
                    Información de comunicaciones (informe completo)

Tipo de objeto . . . . . :   *LIND
                                                          Segs.
 Nombre         Tipo          Categoría      Creación    supres.     Resp.      Marcación
 objeto         objeto         línea         autom.      autom.      autom.     autom.
 LINE01          *LIND         *SDLC           *NO            0       *NO        *NO
 LINE02          *LIND         *SDLC           *NO            0       *YES       *NO
 LINE03          *LIND         *SDLC           *NO            0       *NO        *NO
 LINE04          *LIND         *SDLC           *NO            0       *YES       *NO
```

Figura 12. Descripciones de línea de APPC-Ejemplo de informe

Campo Respuesta automática

El campo Respuesta automática (AUTOANS) indica si la línea conmutada aceptará las llamadas de entrada sin la intervención del operador.

Si se especifica *YES, el sistema será menos seguro, ya que se podrá acceder a él con más facilidad. Para reducir los riesgos de seguridad cuando se especifica *YES, debe desactivar la línea cuando no sea necesaria.

Campo Marcación automática

El campo Marcación automática (AUTODIAL) especifica si la línea conmutada puede realizar llamadas de salida sin la intervención del operador.Si se especifica *YES, se permite a los usuarios locales que no tienen acceso físico a los módems y a las líneas de comunicaciones que se conecten a otros sistemas.

Capítulo 13. Protección de las comunicaciones TCP/IP

TCP/IP (Protocolo de control de transmisión/Protocolo de Internet) es una forma habitual de comunicación entre sistemas informáticos de todo tipo. Las aplicaciones TCP/IP son bien conocidas y ampliamente utilizadas a lo largo de las "autopistas de la información".

En este capítulo se proporcionan consejos para lo siguiente:

- Evitar la ejecución de aplicaciones TCP/IP en el sistema.
- Proteger los recursos del sistema cuando se permite la ejecución de aplicaciones TCP/IP en él.

El sitio Web iSeries Information Center—>Redes—>TCP/IP es la fuente de información más completa sobre todas las aplicaciones TCP/IP. *SecureWay: iSeries e Internet* (iSeries Information Center—>Seguridad—>SecureWay describe las consideraciones sobre la seguridad al conectar el servidor iSeries a Internet (una red TCP/IP de gran tamaño) o a una intranet. Consulte "Requisitos e información relacionada" en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Recuerde que los servidores iSeries dan soporte a muchas aplicaciones TCP/IP posibles. Cuando decide permitir una aplicación TCP/IP en el sistema, puede que también esté permitiendo otras aplicaciones TCP/IP. Como administrador de seguridad, necesita conocer el alcance de las aplicaciones TCP/IP y las implicaciones de seguridad de estas aplicaciones.

Prevención del proceso de TCP/IP

Los trabajos servidores TCP/IP se ejecutan en el subsistema QSYSWRK. Se utiliza el mandato Arrancar TCP/IP (STRTCP) para arrancar TCP/IP en el sistema. Si no quiere ejecutar ningún proceso ni aplicación TCP/IP, no utilice el mandato STRTCP. El sistema se suministra con el valor *EXCLUDE para la autorización de uso público para el mandato STRTCP.

Si sospecha que alguien con acceso al mandato está arrancando TCP/IP (fuera de horas de trabajo, por ejemplo), puede establecer la auditoría de objetos sobre el mandato STRTCP. El sistema grabará una entrada de diario de auditoría cada vez que un usuario ejecute el mandato.

Componentes de la seguridad de TCP/IP

Puede beneficiarse de diversos componentes de seguridad de TCP/IP que mejoran la seguridad de la red y añaden flexibilidad. Aunque algunas de estas tecnologías también se encuentran en productos cortafuegos, estos componentes de seguridad de TCP/IP para OS/400 no están pensados para utilizarlos como cortafuegos. No obstante, puede utilizar algunas de sus funciones, en algunos casos para eliminar la necesidad de un producto cortafuegos aparte. También puede utilizar estas funciones TCP/IP para proporcionar una seguridad adicional a los entornos en los que ya se esté utilizando un cortafuegos.

Los siguientes componentes pueden utilizarse para mejorar la Seguridad de TCP/IP:

- Reglas de paquetes
- Servidor proxy HTTP
- VPN (redes privadas virtuales)
- SSL (capa de sockets segura)

Utilización de reglas de paquetes para asegurar el tráfico de TCP/IP

Las reglas de paquetes, que son la combinación del filtrado de IP y la conversión de direcciones de red (NAT) actúa como un cortafuegos para proteger la red interna ante intrusos. El filtrado de IP le permite controlar qué tráfico de IP va a entrar y salir de su red. Básicamente, protege la red filtrando los paquetes según las reglas que defina. Por otro lado, NAT le permite ocultar sus direcciones IP privadas no registradas tras un conjunto de direcciones IP registradas. Esto ayuda a proteger la red interna de las redes externas. NAT también ayuda a aliviar el problema de despliegue de direcciones IP, ya que muchas direcciones privadas pueden estar representadas por un conjunto pequeño de direcciones registradas. Consulte iSeries Information Center para obtener más detalles.

Servidor proxy HTTP

El servidor proxy HTTP viene con el servidor IBM HTTP para el servidor iSeries. El servidor HTTP forma parte de OS/400. El servidor proxy recibe las peticiones HTTP de los navegadores Web, y las vuelve a enviar a los servidores Web. Los servidores Web que reciben las peticiones solamente conocen las direcciones IP del servidor proxy, y no pueden determinar los nombres o direcciones de los PC que originaron las peticiones. El servidor proxy puede manejar peticiones URL para HTTP, FTP, Gopher y WAIS.

El servidor proxy pone en antememoria las páginas Web devueltas, consecuencia de las peticiones efectuadas por todos los usuarios del servidor proxy. Por lo tanto, cuando los usuarios pidan una página, el servidor proxy comprobará su existencia en la antememoria. En caso afirmativo, el servidor proxy devolverá la página que tiene en la antememoria. Con el uso de páginas en antememoria, el servidor proxy es capaz de servir páginas Web con más rapidez, lo cual elimina las peticiones al servidor Web que potencialmente podrían consumir mucho tiempo.

El servidor proxy también puede anotar todas las peticiones URL a efectos de rastreo. Posteriormente se pueden repasar las anotaciones para supervisar el uso y mal uso de los recursos de la red.

Puede utilizar el soporte de proxy HTTP del IBM HTTP Server para consolidar el acceso a la Web. Las direcciones de los clientes PC se ocultan a los servidores Web a los que acceden; solamente se conoce la dirección IP del servidor proxy. Poner en antememoria las páginas Web también reduce los requisitos de ancho de banda en las comunicaciones y la carga de trabajo de los cortafuegos. Consulte la página de presentación de IBM HTTP Server for iSeries para obtener más información: http://www-1.ibm.com/servers/eserver/iseries/software/http/index.html

Redes privadas virtuales (VPN)

Una red privada virtual (VPN) permite a su empresa ampliar de forma segura su intranet privada por la infraestructura existente de una red pública como Internet. Con VPN, su empresa puede controlar el tráfico de la red a la vez que proporciona importantes funciones de seguridad como la autenticación y la privacidad de los datos.

OS/400 VPN es un componente instalable de forma opcional de iSeries Navigator, la interfaz gráfica de usuario (GUI) de OS/400. Le permite crear una ruta segura de un extremo a otro de cualquier combinación de sistema principal y pasarela. OS/400 VPN utiliza métodos de autenticación, algoritmos de cifrado y otras precauciones para asegurar que los datos enviados entre los dos puntos finales de la conexión permanecen protegidos.

VPN se ejecuta en la capa de red del modelo de pila de comunicaciones por capas de TCP/IP. Concretamente, VPN utiliza la infraestructura abierta de IP Security Architecture (IPSec). IPSec proporciona funciones de seguridad básicas para Internet y proporciona también bloques de construcción flexibles, a partir de los cuales puede crear redes privadas virtuales sólidas y seguras.

VPN también da soporte a soluciones VPN Layer 2 Tunnel Protocol (L2TP). Las conexiones L2TP, también denominadas líneas virtuales, proporcionan acceso económico para los usuarios remotos permitiendo a un servidor de red corporativa gestionar las direcciones IP asignadas a sus usuarios remotos. Además, las conexiones L2TP proporcionan un acceso seguro a su sistema o red al protegerlos con IPSec.

Es importante comprender la repercusión que una VPN puede tener en toda la red. Una planificación e implementación correctas son esenciales para tener éxito. Debería repasar el tema VPN en iSeries Information Center para asegurarse de que sabe cómo funcionan las VPN y cómo puede utilizarlas. Para obtener más información, consulte iSeries Information Center—>Seguridad—>Redes privadas virtuales. Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Capa de Sockets Segura (SSL)

La Capa de Sockets Segura (SSL) se ha convertido en un estándar industrial para la habilitación de aplicaciones para sesiones de comunicaciones seguras a través de una red desprotegida como Internet. El protocolo SSL establece conexiones seguras entre aplicaciones de cliente y servidor que proporcionan la autenticación de uno o ambos puntos finales de la sesión de comunicaciones. SSL también proporciona privacidad e integridad de los datos que las aplicaciones de cliente y servidor intercambian. Para obtener más información, consulte iSeries Information Center–>Seguridad—>Capa de Sockets Segura (SSL). Consulte “Requisitos e información relacionada” en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Protección del entorno TCP/IP

Este tema proporciona sugerencias generales acerca de los pasos que puede seguir para reducir los riesgos en la seguridad relativos al entorno TCP/IP del sistema. Estos consejos se aplican a todo el entorno TCP/IP en lugar de a las aplicaciones específicas que se tratan en los temas siguientes.

- Al escribir una aplicación para un puerto TCP/IP, asegúrese de que la aplicación sea adecuadamente segura. Debe tener en cuenta que un extraño podría intentar acceder a dicha aplicación a través de dicho puerto. Un usuario con conocimientos puede intentar efectuar TELNET con la aplicación.
- Supervise la utilización de los puertos de TCP/IP del sistema. Una aplicación de usuario asociada a un puerto TCP/IP puede proporcionar una entrada “trasera” al sistema sin necesidad de ID de usuario o de contraseña. Alguien con la suficiente autoridad en el sistema puede asociar una aplicación con un puerto TCP o UDP.

- Como administrador de seguridad, debe tener en cuenta una técnica llamada *suplantación de IP* utilizada por los piratas informáticos. Cada sistema de una red TCP/IP tiene una dirección IP. Alguien que utilice esta técnica prepara un sistema (normalmente un PC) como si fuera una dirección IP existente o una dirección IP de confianza. Así, el impostor puede establecer una conexión con el sistema haciéndose pasar por un sistema con el que la conexión es habitual.

  Si ejecuta TCP/IP en el sistema y éste participa en una red que no está protegida físicamente (todas las líneas no conmutadas y los enlaces predefinidos), será vulnerable a la suplantación de IP. Para proteger el sistema del daño causado por algún "suplantador", empiece por las sugerencias de este capítulo, tales como la protección de inicio de sesión y la seguridad de objeto. Debe también asegurarse de que el sistema tenga establecidos límites de almacenamiento auxiliar razonables. Esto evita que quien realiza la suplantación inunde el sistema con correo o archivos en spool hasta que el sistema se vuelva inoperante.

  Además, debe supervisar regularmente la actividad de TCP/IP en el sistema. Si detecta la técnica de suplantación de IP, puede intentar descubrir los puntos débiles de la configuración de TCP/IP y hacer ajustes.
- Para la intranet (red de sistemas que no necesitan conectarse directamente con el exterior), utilice las direcciones IP reutilizables. Las direcciones reutilizables están destinadas a ser utilizadas en una red privada. La red troncal de Internet no direcciona los paquetes que tienen una dirección IP reutilizable. Por lo tanto, las direcciones reutilizables proporcionan una capa añadida de protección dentro del cortafuegos.

  El sitio Web iSeries Information Center—>Redes—>TCP/IP proporciona más información sobre cómo se asignan las direcciones IP y sobre los rangos de direcciones IP, así como información de seguridad sobre TCP/IP.
- Si está pensando en conectar el sistema a Internet o a una intranet, revise la información de seguridad de *SecureWay: iSeries e Internet* (iSeries Information Center—>Seguridad—>SecureWay). Consulte "Requisitos e información relacionada" en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Control de los servidores TCP/IP que se inician automáticamente

Como administrador de seguridad, necesita controlar las aplicaciones TCP/IP que se inician automáticamente al iniciar TCP/IP. Hay dos mandatos disponibles para iniciar TCP/IP. Para cada mandato, el sistema utiliza un método distinto para determinar las aplicaciones (servidores) a iniciar.

En la Tabla 22 en la página 133 se muestran ambos mandatos y las recomendaciones de seguridad correspondientes. En la Tabla 23 en la página 133 se muestran los valores de inicio automático para los servidores. Para cambiar el valor de inicio automático para un servidor, utilice el mandato CHGxxxA (Cambiar atributos xxx) para el servidor. Por ejemplo, el mandato para TELNET es CHGTELNA.

Tabla 22. Cómo determinan los mandatos de TCP/IP qué servidores deben iniciarse

Mandato	Qué servidores se inician	Recomendaciones de seguridad
Iniciar TCP/IP (STRTCP)	El sistema inicia todo servidor que especifique AUTOSTART(*YES). La Tabla 23 muestra el valor suministrado para cada servidor TCP/IP.	• Asigne la autorización especial *IOSYSCFG con cuidado para controlar quién puede cambiar los valores de inicio automático. • Controle cuidadosamente quién tiene autorización para utilizar el mandato STRTCP. La autorización de uso público por omisión para el mandato es *EXCLUDE. • Establezca la auditoría de objetos para los mandatos Cambiar atributos de *nombre de servidor* (por ejemplo, CHGTELNA) para supervisar los usuarios que intentan cambiar el valor AUTOSTART para un servidor.
Iniciar servidor TCP/IP (STRTCPSVR)	Debe utilizarse un parámetro para especificar los servidores a iniciar. El valor por omisión al emitir el mandato supone iniciar todos los servidores.	• Utilice el mandato Cambiar valor por omisión de mandato (CHGCMDDFT) para establecer que el mandato STRTCPSVR inicie solamente un servidor determinado. Esto no impide que los usuarios inicien otros servidores. Sin embargo, al cambiar el valor por omisión del mandato, es menos probable que los usuarios inicien todos los servidores accidentalmente. Por ejemplo, utilice el mandato siguiente para que el valor por omisión suponga iniciar sólo el servidor TELNET: `CHGCMDDFT CMD(STRTCPSVR) NEWDFT('SERVER(*TELNET)')` **Nota:** Al cambiar el valor por omisión, puede especificar solamente un único servidor. Elija un servidor que utilice habitualmente o un servidor que implique una menor probabilidad de ser causa de riesgos en la seguridad (como TFTP). • Controle cuidadosamente quién tiene autorización para utilizar el mandato STRTCPSVR. La autorización de uso público por omisión para el mandato es *EXCLUDE.

La tabla siguiente contiene valores de inicio automático para servidores TCP/IP. Para obtener más información sobre cada uno de estos servidores, consulte iSeries Information Center (**Redes—>TCP/IP**). Consulte “Requisitos e información relacionada” en la página xii para obtener detalles sobre cómo acceder a iSeries Information Center.

Tabla 23. Valores de inicio automático para servidores TCP/IP

Servidor	Valor por omisión	Su valor
TELNET	AUTOSTART(*YES)	
FTP (protocolo de transferencia de archivos)	AUTOSTART(*YES)	
BOOTP (Protocolo Bootstrap)	AUTOSTART(*NO)	
TFTP (protocolo trivial de transferencia de archivos)	AUTOSTART(*NO)	
REXEC (servidor de EXECution remoto)	AUTOSTART(*NO)	
RouteD (Daemon de ruta)	AUTOSTART(*NO)	
SMTP (protocolo simple de transferencia de correo)	AUTOSTART(*YES)	
POP (Protocolo de Oficina Postal)	AUTOSTART(*NO)	

Tabla 23. Valores de inicio automático para servidores TCP/IP (continuación)

Servidor	Valor por omisión	Su valor
HTTP (Protocolo de Transferencia de Hipertexto) [1]	AUTOSTART(*NO)	
ICS (Internet Connection Server)[1]	AUTOSTART(*NO)	
LPD (daemon de impresora de líneas)	AUTOSTART(*YES)	
SNMP (Protocolo Simple de Gestión de Correo (SNMP))	AUTOSTART(*YES)	
DNS (sistema de nombres de dominio (DNS))	AUTOSTART(*NO)	
DDM	AUTOSTART(*NO)	
DHCP (Protocolo de configuración dinámica de sistema principal (DHCP))	AUTOSTART(*NO)	
NSMI	AUTOSTART(*NO)	
INETD	AUTOSTART(*NO)	

Notas:

1. En el servidor IBM HTTP para el servidor iSeries, se utiliza el mandato CHGHTTPA para establecer el valor AUTOSTART.

Consideraciones de seguridad para utilizar SLIP

El soporte de TCP/IP del servidor iSeries incluye el Protocolo de Línea de Interfaz Serie (SLIP). SLIP proporciona conectividad punto a punto de bajo coste. Un usuario de SLIP puede conectarse a una LAN o a una WAN estableciendo una conexión punto a punto con un sistema que forme parte de una LAN o una WAN.

SLIP se ejecuta en una conexión asíncrona. Puede utilizar SLIP para efectuar conexiones de marcación a y desde servidores iSeries. Por ejemplo, puede utilizar SLIP para marcar desde el PC a un sistema iSeries. Después de establecer la conexión, puede utilizar la aplicación TELNET en el PC para conectarse al servidor TELNET del iSeries. O puede utilizar la aplicación FTP para transferir archivos entre los dos sistemas.

No existe ninguna configuración de SLIP en el sistema cuando se envía. Por lo tanto, si no quiere que se ejecute SLIP (y TCP/IP de marcación) en el sistema, no configure perfiles para SLIP. Puede utilizar el mandato Trabajar con punto a punto TCP/IP (WRKTCPPTP) para crear configuraciones de SLIP. Debe tener autorización especial *IOSYSCFG para utilizar el mandato WRKTCPPTP.

Si quiere que SLIP se ejecute en el sistema, cree uno o varios perfiles de configuración SLIP (punto a punto). Puede crear perfiles de configuración con las modalidades operativas siguientes:
- Marcación de entrada (*ANS)
- Marcación de salida (*DIAL)

En los temas siguientes se trata la forma de establecer la seguridad para los perfiles de configuración de SLIP.

Nota: Un **perfil de usuario** es un objeto del servidor iSeries que permite iniciar la sesión. Cada trabajo de un servidor iSeries debe tener un perfil de usuario para ejecutarse. Un **perfil de configuración** almacena información que se utiliza para establecer una conexión SLIP con un sistema iSeries. Cuando se arranca una conexión SLIP a servidores iSeries, simplemente se está estableciendo un enlace. Aún no se ha iniciado la sesión ni se ha arrancado un trabajo de servidor iSeries. Por lo tanto no necesita imperativamente un perfil de usuario para arrancar una conexión SLIP a servidores iSeries. Sin embargo, tal como verá en los comentarios siguientes, el perfil de configuración de SLIP puede necesitar un perfil de usuario para determinar si se permite la conexión.

Control de conexiones de marcación SLIP

Para que alguien pueda establecer una conexión de marcación de entrada con el sistema mediante SLIP, debe usted arrancar un perfil de configuración *ANS de SLIP. Para crear o cambiar un perfil de configuración de SLIP, utilice el mandato Trabajar con punto a punto de TCP/IP (WRKTCPPTP). Para arrancar un perfil de configuración, utilice el mandato Arrancar punto a punto de TCP/IP (STRTCPPTP) o una opción de la pantalla WRKTCPPTP. Cuando el sistema se envía, la autorización de uso público para los mandatos STRTCPPTP y ENDTCPPTP es *EXCLUDE. Las opciones añadir, cambiar y suprimir perfiles de configuración de SLIP están disponibles sólo si tiene autorización especial *IOSYSCFG. Como administrador de seguridad, puede utilizar la autorización de mandatos, y la autorización especial, para determinar quién puede configurar el sistema para permitir conexiones de marcación de entrada.

Seguridad de una conexión SLIP de marcación de entrada

Si desea validar los sistemas que efectúen una marcación de entrada en el sistema, querrá que el sistema peticionario envíe un ID de usuario y una contraseña. Su sistema puede entonces verificar el ID de usuario y la contraseña. Si el ID de usuario y la contraseña no son válidos, el sistema puede rechazar la petición de sesión.

Para establecer la validación de la marcación de entrada haga lo siguiente:

__ Paso 1. Cree un perfil de usuario que el sistema peticionario pueda utilizar para establecer la conexión. El ID de usuario y la contraseña que envía el peticionario deben coincidir con este nombre de perfil y esta contraseña.

Nota: Para que el sistema lleve a cabo la validación de la contraseña el valor del sistema QSECURITY debe ser 20 o un valor superior.

Como protección adicional, probablemente querrá crear perfiles de usuario específicos para establecer conexiones SLIP. Los perfiles de usuario deben tener autorización limitada sobre el sistema. Si no va a utilizar los perfiles para ninguna función excepto para establecer conexiones SLIP, puede establecer los valores siguientes en los perfiles de usuario:

- Un menú inicial (INLMNU), *SIGNOFF
- Un programa inicial (INLPGM), *NONE.
- Limitar posibilidades (LMTCPB), *YES

Estos valores impiden que alguien inicie una sesión interactivamente con el perfil de usuario.

__ Paso 2. Cree una lista de autorizaciones para que el sistema haga una comprobación cuando un peticionario intenta establecer una conexión SLIP.

Nota: Esta lista de autorizaciones se especifica en el campo *Lista de autorizaciones de acceso al sistema*, al crear o modificar el perfil de SLIP. (Vea el paso 4.)

__ Paso 3. Utilice el mandato Añadir entrada de autorización (ADDAUTLE) para añadir el perfil de usuario creado en el paso 1 a la lista de autorizaciones. Puede crear una lista de autorizaciones exclusiva para cada perfil de configuración punto a punto, o puede crear una lista de autorizaciones que compartan varios perfiles de configuración.

__ Paso 4. Utilice el mandato WRKTCPPTP para establecer un perfil *ANS punto a punto de TCP/IP que tenga las características siguientes:

- El perfil de configuración debe utilizar un script de diálogo que incluya la función de validación del usuario. La validación del usuario incluye la aceptación de un ID de usuario y de una contraseña del peticionario y su validación. El sistema se envía con varios scripts de diálogo de ejemplo que proporcionan esta función.
- El perfil de configuración debe especificar el nombre de la lista de autorizaciones creada en el paso 2. El ID de usuario que recibe el script de diálogo de conexión debe estar en la lista de autorizaciones.

Tenga en cuenta que el valor de configuración de la seguridad de marcación se ve afectado por las posibilidades y las prácticas de seguridad de los sistemas que efectúan la marcación de entrada. Si necesita un ID de usuario y una contraseña, el script de diálogo de conexión del sistema peticionario debe enviar el ID de usuario y la contraseña. Algunos sistemas, como los servidores iSeries, proporcionan un método seguro para almacenar los ID de usuario y las contraseñas. (Este método se describe en el apartado "Seguridad y sesiones de marcación de salida" en la página 137). Otros sistemas almacenan el ID de usuario y la contraseña en un script que puede ser accesible a cualquiera que sepa donde encontrarlo en el sistema.

Debido a las diferentes posibilidades y prácticas en materia de seguridad de los comunicantes, querrá crear diferentes perfiles de configuración para diferentes entornos de petición. Puede utilizar el mandato STRTCPPTP para configurar el sistema para aceptar una sesión para un perfil de configuración específico. Para algunos perfiles de configuración puede arrancar sesiones sólo en determinados momentos del día, por ejemplo. Puede utilizar la auditoría de seguridad para llevar un registro de anotaciones cronológicas de la actividad de los perfiles de usuario asociados.

Evitar que los usuarios de marcación accedan a otros sistemas

Dependiendo del sistema y de la configuración de red, un usuario que arranque una conexión SLIP puede ser capaz de acceder a otro sistema en la red sin iniciar la sesión en el sistema. Por ejemplo, un usuario podría establecer una conexión SLIP con el sistema. A continuación, el usuario podría establecer una conexión FTP con otro sistema de la red que no permita entrar por una línea telefónica.

Puede evitar que un usuario SLIP acceda a otros sistemas de la red especificando N (No) para el campo *Permitir reenvío de datagramas IP* en el perfil de configuración. Esto impide que un usuario acceda a la red antes de que inicie sesión en su sistema. Sin embargo, una vez que el usuario haya iniciado la sesión

de forma satisfactoria en el sistema, el valor de reenvío de datagramas no tiene efecto. No limita la capacidad del usuario para utilizar una aplicación TCP/IP en el sistema iSeries (por ejemplo, FTP o TELNET), para establecer una conexión con otro sistema de la red.

Control de las sesiones de marcación de salida

Antes de que alguien pueda utilizar SLIP para establecer una conexión de marcación de salida desde el sistema, debe arrancar un perfil de configuración *DIAL de SLIP. Para crear o cambiar un perfil de configuración SLIP, utilice el mandato WRKTCPPTP. Para arrancar un perfil de configuración, utilice el mandato Arrancar punto a punto de TCP/IP (STRTCPPTP) o una opción de la pantalla WRKTCPPTP. Cuando el sistema se envía, la autorización de uso público para los mandatos STRTCPPTP y ENDTCPPTP es *EXCLUDE. Las opciones añadir, cambiar y suprimir perfiles de configuración de SLIP están disponibles sólo si tiene autorización especial *IOSYSCFG. Como administrador de seguridad, puede utilizar la autorización de mandatos y la autorización especial para determinar quién puede configurar el sistema para permitir conexiones de marcación de salida.

Seguridad y sesiones de marcación de salida

Los usuarios del sistema iSeries querrán establecer conexiones de marcación con sistemas que requieran validación de usuario. El script de diálogo de conexión en el servidor iSeries debe enviar un ID de usuario y una contraseña al sistema remoto. Los servidores iSeries proporcionan un método seguro para almacenar la contraseña. No es necesario almacenar la contraseña en el script de diálogo de conexión.

Notas:

1. A pesar de que el sistema almacena la contraseña de conexión de forma cifrada, el sistema la descifra antes de enviarla. Las contraseñas de SLIP, igual que las contraseñas de FTP y TELNET, se envían descifradas. Sin embargo, al contrario que con FTP y TELNET, la contraseña SLIP se envía antes de que los sistemas establezcan la modalidad TCP/IP.

   Puesto que SLIP utiliza una conexión punto a punto en la modalidad asíncrona, el riesgo en la seguridad al enviar contraseñas no cifradas es distinto del riesgo con las contraseñas FTP y TELNET. Las contraseñas no cifradas de FTP y TELNET pueden enviarse como tráfico IP en una red y son, por tanto, vulnerables a la búsqueda electrónica. La transmisión de la contraseña SLIP es tan segura como lo sea la conexión telefónica entre ambos sistemas.
2. El archivo por omisión para almacenar los scripts de diálogo de conexión SLIP es QUSRSYS/QATOCPPSCR. La autorización de uso público para este archivo es *USE, lo que evita que los usuarios públicos cambien los scripts de diálogo de conexión por omisión.

Cuando crea un perfil de conexión para una sesión remota que necesite validación, haga lo siguiente:

__ Paso 1. Asegúrese de que el valor del sistema Retener datos de seguridad del servidor (QRETSVRSEC) es 1 (Sí). Este valor del sistema determina si permitirá que las contraseñas que pueden descifrarse se almacenen en un área protegida de su sistema.

__ Paso 2. Utilice el mandato WRKTCPPTP para crear un perfil de configuración que tenga las características siguientes:

- Para la modalidad del perfil de configuración, especifique *DIAL.

- Para el *Nombre de acceso de servicio remoto*, especifique el ID de usuario que el sistema remoto espera. Por ejemplo, si va a conectarse con otro servidor iSeries, especifique el nombre del perfil de usuario en ese servidor iSeries.
- Para la *Contraseña de acceso de servicio remoto*, especifique la contraseña que el sistema remoto espera para este ID de usuario. En su servidor iSeries, esta contraseña se almacena en un área protegida en un formato que puede descifrarse. Los nombres y las contraseñas que asigna a los perfiles de configuración están asociados con el perfil de usuario de QTCP. Los nombres y las contraseñas no son accesibles con ninguna interfaz o mandato de usuario. Sólo los programas registrados del sistema pueden acceder a esta información de contraseña.

  Nota: Tenga en cuenta que las contraseñas para sus perfiles de conexión no se salvan al salvar los archivos de configuración de TCP/IP. Para salvar las contraseñas SLIP, necesita utilizar el mandato Salvar datos de seguridad (SAVSECDTA) para salvar el perfil de usuario QTCP.
- Para el script de diálogo de conexión, especifique un script que envíe el ID de usuario y la contraseña. El sistema se envía con varios scripts de diálogo de ejemplo que proporcionan esta función. Cuando el sistema ejecuta el script, recupera la contraseña, la descifra y la envía al sistema remoto.

Consideraciones de seguridad para el protocolo punto a punto

El protocolo punto a punto (PPP) está disponible como parte de TCP/IP. PPP es un estándar comercial para las conexiones punto a punto que proporciona funciones adicionales sobre lo que está disponible con SLIP.

Con PPP, el servidor iSeries puede tener conexiones de alta velocidad directamente con un proveedor de servicios de Internet o con otros sistemas de una intranet o una extranet. Las LAN remotas pueden realmente conectarse mediante marcación al servidor iSeries.

Recuerde que PPP, al igual que SLIP, proporciona una conexión de red al servidor iSeries. Esencialmente, una conexión PPP trae al peticionario a la puerta del sistema. El peticionario sigue necesitando un ID de usuario y una contraseña para entrar en el sistema y conectarse a un servidor TCP/IP como TELNET o FTP. A continuación se proporcionan algunas consideraciones de seguridad con esta nueva posibilidad de conexión:

Nota: PPP se configura utilizando iSeries Navigator en una estación de trabajo IBM iSeries Access para Windows.

- PPP proporciona la posibilidad de tener conexiones dedicadas (en las que el mismo usuario tiene siempre la misma dirección IP). Con una dirección dedicada, tiene el potencial para suplantación de IP (un sistema impostor que pretende hacerse pasar por un sistema de confianza con una dirección IP conocida). Sin embargo, las posibilidades de autenticación mejoradas que proporciona PPP ayudan en la protección contra la suplantación de IP.
- Con PPP, al igual que con SLIP, puede crear perfiles de conexión que tienen un nombre de usuario y una contraseña asociada. No obstante, al contrario que con SLIP, el usuario no necesita tener un perfil de usuario y contraseña válidos. El nombre de usuario y la contraseña no están asociados con un perfil de usuario,

sino que se utilizan listas de validación para la autenticación de PPP. Además, PPP no requiere un script de conexión. La autenticación (intercambio de nombre de usuario y contraseña) es parte de la arquitectura PPP y transcurre a un nivel más bajo que en el caso de SLIP.

- Con PPP tiene la opción de utilizar CHAP (challenge handshake authentication protocol). Ya no necesitará preocuparse acerca de si existen escuchas ocultas en busca de contraseñas porque CHAP cifra los nombres de usuario y las contraseñas.

  La conexión PPP utiliza CHAP solamente si ambas partes tienen soporte CHAP. Durante las señales de intercambio para establecer las comunicaciones entre dos módems, los dos sistemas negocian. Por ejemplo, si SYSTEMA soporta CHAP y SYSTEMB no, SYSTEMA puede denegar la sesión o avenirse a utilizar un nombre de usuario y una contraseña no cifrados. Aceptar la utilización de un nombre de usuario y de una contraseña no cifrados significa negociar a la baja. La decisión de negociar a la baja es una opción de configuración. En la intranet, por ejemplo, donde sabe que todos los sistemas tienen posibilidad CHAP, debe configurar el perfil de conexión de forma que no negocie a la baja. En una conexión de uso público donde el sistema está marcando fuera, puede ser deseable negociar a la baja.

  El perfil de conexión para PPP proporciona la posibilidad de especificar direcciones IP válidas. Puede, por ejemplo, indicar que espera una dirección o un rango de direcciones específicos para un usuario determinado. Esta posibilidad, conjuntamente con la capacidad para contraseñas cifradas, proporciona una mayor protección contra la suplantación.

  Como protección adicional contra la suplantación o el parasitismo en una sesión activa, puede configurar PPP para que pida confirmación a intervalos establecidos. Por ejemplo, mientras una sesión PPP está activa, el servidor iSeries puede pedir al otro sistema un usuario y una contraseña.Esto lo hace cada 15 minutos para asegurarse de que se trata del mismo perfil de conexión. (El usuario final no se dará cuenta de la existencia de esta actividad de confirmación. Los sistemas intercambian los nombres y las contraseñas por debajo del nivel que ve el usuario final.)

  Con PPP, es realista esperar que las LAN remotas puedan establecer una conexión por marcación con el servidor iSeries y con la red ampliada. En este entorno, probablemente sea un requisito tener activado el reenvío de IP. El reenvío de IP tiene el potencial para permitir a un intruso vagar por la red. Sin embargo, PPP tiene protecciones más potentes (como el cifrado de contraseñas y la validación de la dirección IP). Esto convierte en menos probable el que un intruso pueda establecer una conexión de red en primer lugar.

Para obtener más información sobre PPP, consulte iSeries Information Center.

Consideraciones de seguridad para utilizar el servidor Protocolo Bootstrap

El Protocolo Bootstrap (BOOTP) proporciona un método dinámico para asociar estaciones de trabajo a servidores y para asignar direcciones IP de estación de trabajo y recursos de carga del programa inicial (IPL).

BOOTP es un protocolo TCP/IP que se utiliza para permitir que una estación de trabajo sin ningún tipo de soporte de almacenamiento (cliente) solicite un archivo que contenga un código inicial de un servidor de la red. El servidor BOOTP escucha al puerto 67 del servidor BOOTP. Al recibir una petición de un cliente, el servidor busca la dirección IP definida para el cliente y le devuelve una respuesta

con la dirección IP del cliente y el nombre del archivo de carga. A continuación, el cliente inicia una petición TFTP al servidor solicitando el archivo de carga. La correlación entre la dirección IP y la dirección de hardware del cliente se conserva en la tabla BOOTP del servidor iSeries.

Impedir el acceso a BOOTP

Si no tiene clientes ligeros conectados a la red, no es necesario ejecutar el servidor BOOTP en su sistema. Puede utilizarse para otros dispositivos, pero la solución preferida para esos dispositivos es utilizar DHCP. Para evitar que se ejecute el servidor BOOTP, haga lo siguiente:

__ Paso 1. Para evitar que los trabajos del servidor BOOTP se inicien automáticamente al arrancar TCP/IP, teclee lo siguiente:

```
CHGBPA AUTOSTART(*NO)
```

Notas:

a. AUTOSTART(*NO) es el valor por omisión.

b. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

__ Paso 2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para BOOTP, haga lo siguiente:

Nota: Dado que DHCP y BOOTP utilizan el mismo número de puerto, esto también inhibirá el puerto que DHCP utiliza. No debe restringir el puerto si desea utilizar DHCP.

__ Paso a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.

__ Paso b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).

__ Paso c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).

__ Paso d. Para el rango del puerto más bajo, especifique `67`.

__ Paso e. Para el rango del puerto más alto, especifique `*ONLY`.

Notas:

1) La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.

2) RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

__ Paso f. Para el protocolo, especifique `*UDP`.

__ Paso g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.

Protección del servidor BOOTP

El servidor BOOTP no proporciona acceso directo para su sistema iSeries y, por consiguiente, representa un riesgo de seguridad limitado. Su preocupación principal como administrador de seguridad es asegurarse de que la información correcta se asocie al cliente ligero correcto. En otras palabras, una persona malintencionada podría modificar la tabla BOOTP y hacer que los clientes ligeros no funcionaran o funcionaran incorrectamente.

Para administrar el servidor BOOTP y la tabla BOOTP, debe disponer de la autorización especial *IOSYSCFG. Debe controlar cuidadosamente los perfiles de usuario que tienen la autorización especial *IOSYSCFG en su sistema.

Consideraciones de seguridad para utilizar el servidor DHCP

Protocolo de configuración dinámica de sistema principal (DHCP) proporciona una infraestructura para pasar información de configuración a los sistemas principales en una red TCP/IP. Para las estaciones de trabajo clientes, DHCP puede proporcionar una función similar a la configuración automática. Un programa habilitado para DHCP en la estación de trabajo cliente difunde una petición de información de configuración. Si el servidor DHCP está ejecutándose en el servidor iSeries, el servidor responde a la petición enviando la información que necesita la estación de trabajo cliente para configurar correctamente TCP/IP.

Puede utilizar DHCP para que sea más sencillo para los usuarios conectarse al servidor iSeries por primera vez. Esto obedece a que el usuario no necesita especificar información de configuración de TCP/IP. También puede utilizar DHCP para reducir el número de direcciones internas de TCP/IP que necesita en una subred. El servidor DHCP puede asignar temporalmente direcciones IP a usuarios activos (de su agrupación de direcciones IP).

Para los clientes ligeros puede utilizar DHCP en lugar de BOOTP. DHCP proporciona más funciones que BOOTP y puede dar soporte a la configuración dinámica de clientes ligeros y de PC.

Impedir el acceso a DHCP

Si *no* quiere que nadie utilice el servidor DHCP en el sistema, lleve a cabo lo siguiente:

1. Para evitar que los trabajos del servidor DHCP se inicien automáticamente al arrancar TCP/IP, teclee lo siguiente:

   ```
   CHGDHCPA AUTOSTART(*NO)
   ```

   Notas:

   a. AUTOSTART(*NO) es el valor por omisión.

   b. “Control de los servidores TCP/IP que se inician automáticamente” en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para DHCP, haga lo siguiente:

   a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.

   b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).

   c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).

d. Para el rango del puerto más bajo, especifique 67.
e. Para el rango del puerto más alto, especifique 68.

Notas:

1) La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.
2) RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

f. Para el protocolo, especifique *UDP.
g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.

Protección del servidor DHCP

A continuación se proporcionan una serie de consideraciones de seguridad que debe tener en cuenta al ejecutar DHCP en el sistema iSeries:

- Restrinja el número de usuarios con autoridad para administrar DHCP. La administración de DHCP requiere la autorización siguiente:
  - Autorización especial *IOSYSCFG
  - Autorización *RW sobre los archivos siguientes:

    ```
    /QIBM/UserData/OS400/DHCP/dhcpsd.cfg
    /QIBM/UserData/OS400/DHCP/dhcprd.cfg
    ```
- Evalúe la accesibilidad física de la LAN. ¿Podría un extraño entrar fácilmente en sus instalaciones con un portátil y conectarse físicamente a la LAN? Si esto constituye un riesgo, DHCP proporciona la posibilidad de crear una lista de clientes (direcciones de hardware) que configurará el servidor DHCP. Al utilizar esta característica, se elimina parte de la mejora en la productividad que DHCP proporciona a los administradores de red. Sin embargo, se está evitando que el sistema configure estaciones de trabajo desconocidas.
- Si es posible, utilice una agrupación de direcciones IP que sea reutilizable (no estructurada para Internet). Esto contribuye a evitar que una estación de trabajo externa a la red obtenga del servidor información de configuración utilizable.
- Utilice los puntos de salida de DHCP si necesita protección de seguridad adicional. A continuación se proporciona una visión general de los puntos de salida y de las posibilidades de los mismos. La publicación *iSeries System API Reference* describe cómo utilizar estos puntos de salida.

  Entrada de puerto
  El sistema llama al programa de salida siempre que lee un paquete de datos del puerto 67 (el puerto de DHCP). El programa de salida recibe el paquete de datos completo. El programa de salida puede decidir si el sistema debe procesar o descartar el paquete. Puede utilizar este punto de salida cuando las características de protección de DHCP no sean suficientes para sus necesidades.

  Asignación de dirección
  El sistema llama al programa de salida siempre que DHCP asigne formalmente una dirección a un cliente.

Liberación de dirección
El sistema llama al programa de salida siempre que DHCP libera formalmente una dirección y la vuelve a colocar en la agrupación de direcciones.

Consideraciones de seguridad para utilizar el servidor TFTP

El Protocolo trivial de transferencia de archivos (TFTP) proporciona la transferencia básica de archivos sin autenticación de usuario. TFTP trabaja con el Protocolo Bootstrap (BOOTP) o el Protocolo de Configuración Dinámica de Sistema Principal (DHCP) (DHCP).

El cliente se conecta inicialmente al servidor BOOTP o al servidor DHCP. El servidor BOOTP o el servidor DHCP responden con la dirección IP del cliente y el nombre del archivo de carga. A continuación, el cliente inicia una petición TFTP al servidor solicitando el archivo de carga. Cuando el cliente termina de bajar el archivo de carga, finaliza la sesión TFTP.

Impedir el acceso a TFTP

Si no tiene clientes ligeros conectados a la red, probablemente no será necesario ejecutar el servidor TFTP en su sistema. Para evitar que se ejecute el servidor TFTP, haga lo siguiente:

__ Paso 1. Para evitar que los trabajos del servidor TFTP se inicien automáticamente al arrancar TCP/IP, teclee lo siguiente:

```
CHGTFTPA AUTOSTART(*NO)
```

Notas:

a. AUTOSTART(*NO) es el valor por omisión.

b. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

__ Paso 2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para TFTP, haga lo siguiente:

__ Paso a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.

__ Paso b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).

__ Paso c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).

__ Paso d. Para el rango del puerto más bajo, especifique `69`.

__ Paso e. Para el rango del puerto más alto, especifique `*ONLY`.

Notas:

1) La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.

2) RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

__ Paso f. Para el protocolo, especifique `*UDP`.

__ Paso g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles

de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.

Protección del servidor TFTP

Por omisión, el servidor TFTP proporciona acceso muy limitado al sistema iSeries. Se ha configurado específicamente para proporcionar el código inicial para los clientes ligeros. Como administrador de seguridad, debe tener en cuenta las características siguientes del servidor TFTP:

- El servidor TFTP no requiere autenticación (una contraseña y un ID de usuario). Todos los trabajos TFTP se ejecutan bajo el perfil de usuario QTFTP. El perfil de usuario QTFTP no tiene una contraseña. Por consiguiente, no está disponible para el inicio de sesión interactivo. El perfil de usuario QTFTP no tiene ninguna autorización especial, ni tiene ninguna autorización explícita para los recursos del sistema. Utiliza la autorización pública para acceder a los recursos que necesita para los clientes ligeros.
- Cuando se recibe el servidor TFTP, está configurado para acceder al directorio que contiene la información del cliente ligero. Debe tener autorización *PUBLIC o QTFTP debe tener autorización para leer o grabar en ese directorio. Para grabar en el directorio debe haber especificado *CREATE en el parámetro "Permitir grabación en archivo" del mandato CHGTFTPA. Para grabar en un archivo ya existente debe haber especificado *REPLACE en el parámetro "Permitir grabación en archivo" de CHGTFTPA. *CREATE le permite sustituir archivos ya existentes o crear archivos nuevos. *REPLACE solamente le permite sustituir archivos ya existentes.

  Un cliente TFTP no puede acceder a ningún otro directorio a menos que se defina explícitamente en el directorio con el mandato Cambiar atributos TFTP (CHGTFTPA). Por consiguiente, si un usuario local o remoto no intenta iniciar una sesión TFTP para el sistema, la posibilidad del usuario de acceder a la información o causar daños es extremadamente limitada.
- Si elige configurar el servidor TFTP para proporcionar otros servicios, además de manejar clientes ligeros, puede definir un programa de salida para evaluar y autorizar cada petición TFTP. El servidor TFTP proporciona una salida de validación de petición similar a la salida que está disponible para el servidor FTP. Para obtener más información, consulte iSeries Information Center—>Redes—>TCP/IP—>TFTP. Consulte "Requisitos e información relacionada" en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Consideraciones de seguridad para utilizar el servidor REXEC

El servidor de EXECution remoto (REXEC) recibe y ejecuta mandatos de un cliente REXEC. Generalmente, un cliente REXEC es una aplicación de PC o UNIX que soporta el envío de mandatos de REXEC. El soporte que proporciona este servidor es similar a la posibilidad que está disponible al utilizar el submandato RCMD (mandato remoto) para el servidor FTP.

Impedir el acceso a REXEC

Si no desea que el servidor iSeries acepte mandatos de un cliente REXEC, haga lo siguiente para evitar que se ejecute el servidor REXEC:

__ Paso 1. Para evitar que los trabajos del servidor REXEC se inicien automáticamente al iniciar TCP/IP, escriba lo siguiente:

```
CHGRXCA AUTOSTART(*NO)
```

Notas:

a. AUTOSTART(*NO) es el valor por omisión.

b. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

__ Paso 2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para REXEC, haga lo siguiente:

__ Paso a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.

__ Paso b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).

__ Paso c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).

__ Paso d. Para el rango del puerto más bajo, especifique `512`.

__ Paso e. Para el rango del puerto más alto, especifique `*ONLY`.

__ Paso f. Para el protocolo, especifique `*TCP`.

__ Paso g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.

Notas:

a. La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.

b. RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

Protección del servidor REXEC

A continuación se incluyen algunas consideraciones que debe tener en cuenta al elegir la ejecución del servidor de EXECution remoto en su sistema:

- Una petición REXCD incluye un ID de usuario, una contraseña y el mandato a ejecutar. Se aplica la autenticación normal del servidor iSeries y la comprobación de autenticación:
  - La combinación de perfil de usuario y contraseña debe ser válida.
  - El sistema fuerza el valor de *Limitar posibilidades* (LMTCPB) para el perfil de usuario.
  - El usuario debe disponer de autorización para el mandato y para todos los recursos que utiliza el mandato.
- El servidor REXEC proporciona puntos de salida similares a los puntos de salida que están disponibles para el servidor FTP. Puede utilizar el punto de salida de Validación para evaluar el mandato y decidir si se autoriza. Para obtener más información, consulte iSeries Information Center—>Redes—>TCP/IP—>REXEC. Consulte "Requisitos e información relacionada" en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

- Cuando elige ejecutar el servidor REXEC, ejecutará fuera de cualquier control de acceso de menú que tenga en el sistema. Debe asegurarse de que el esquema de autorización de objeto sea el adecuado para la protección de los recursos.

Consideraciones de seguridad para utilizar RouteD

El servidor Daemon de ruta (RouteD) proporciona soporte para RIP (Protocolo de información de direccionamiento) en servidores iSeries. RIP es el protocolo de direccionamiento más utilizado. Se trata de un Protocolo de pasarela interior que ayuda a TCP/IP en el direccionamiento de paquetes IP en un sistema autónomo.

La finalidad de RouteD es aumentar la eficacia del tráfico de red, permitiendo que los sistemas de una red autorizada se actualicen entre sí con la información de ruta actual. Al ejecutar RouteD, su sistema recibe las actualizaciones de los demás sistemas participantes acerca de cómo deben direccionarse las transmisiones (paquetes). Por consiguiente, si los piratas informáticos pueden acceder al servidor RouteD, pueden utilizarlo para redireccionar los paquetes a través de un sistema que puede husmear o modificar los paquetes. A continuación se incluyen algunas sugerencias para la seguridad RouteD:

- Los servidores iSeries utilizan RIPv1, que no proporciona ningún método para la autenticación de direccionadores. Su finalidad es utilizarla dentro de una red autorizada. Si su sistema es una red con otros sistemas en los que no "confía", no debe ejecutar el servidor RouteD. Para garantizar que el servidor RouteD no se inicia automáticamente, escriba lo siguiente:

  ```
  CHGRTDA AUTOSTART(*NO)
  ```

  Notas:

  1. AUTOSTART(*NO) es el valor por omisión.
  2. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.
- Asegúrese de que controla a la persona que cambia la configuración de RouteD, que requiere la autorización especial *IOSYSCFG.
- Si el sistema está presente en más de una red (por ejemplo en una intranet y en Internet), puede configurar el servidor RouteD para enviar y aceptar actualizaciones sólo con la red segura.

Consideraciones de seguridad para utilizar el servidor DNS

El servidor Sistema de nombres de dominio (DNS) proporciona la conversión de un nombre de sistema principal a una dirección IP y viceversa. En los servidores iSeries, el servidor DNS tiene la misión de proporcionar la conversión de direcciones para la red interna segura (intranet).

Impedir el acceso a DNS

Si *no* quiere que nadie utilice el servidor DNS en el sistema, lleve a cabo lo siguiente:

1. Para evitar que los trabajos del servidor DNS se inicien automáticamente al iniciar TCP/IP, escriba lo siguiente:

   ```
   CHGDNSA AUTOSTART(*NO)
   ```

   Notas:

   a. AUTOSTART(*NO) es el valor por omisión.

b. “Control de los servidores TCP/IP que se inician automáticamente” en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para DNS, haga lo siguiente:
   a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.
   b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).
   c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).
   d. Para el rango del puerto más bajo, especifique `53`.
   e. Para el rango del puerto más alto, especifique `*ONLY`.

      Notas:

      1) La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.
      2) RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

   f. Para el protocolo, especifique `*TCP`.
   g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.
   h. Repita los pasos del 2c al 2g para el protocolo *UDP (Datagrama de usuario).

Protección del servidor DNS

A continuación se proporcionan una serie de consideraciones de seguridad que debe tener en cuenta al ejecutar DNS en el sistema iSeries:

- La función que proporciona el servidor DNS es la conversión de direcciones IP y la conversión de nombres. No proporciona acceso a objetos del sistema iSeries.El riesgo que supone el que un extraño acceda al servidor DNS consiste en que el servidor proporciona una forma fácil de ver la topología de la red. El DNS puede ahorrar esfuerzos a los piratas a la hora de determinar las direcciones de los destinos potenciales. Sin embargo, el DNS no proporciona información que ayude a irrumpir en tales sistemas destino.
- Normalmente se utiliza el servidor DNS de iSeries para la intranet. Por lo tanto, probablemente no tenga necesidad de restringir la capacidad de consultar el DNS. Sin embargo, es posible que tenga, por ejemplo, varias subredes en la intranet. Es posible que no desee que los usuarios de otra subred puedan consultar el DNS de su servidor iSeries. Existe una opción de seguridad del DNS que permite limitar el acceso a un dominio primario. Utilice iSeries Navigator para especificar direcciones IP a las que el servidor DNS deberá responder.

  Otra opción de seguridad permite especificar qué servidores secundarios pueden copiar información del servidor DNS primario. Cuando se utiliza esta opción, el servidor aceptará las peticiones de transferencia de zona (una petición para copiar información) solamente de los servidores secundarios listados explícitamente.
- Asegúrese de restringir cuidadosamente la capacidad de cambiar el archivo de configuración del servidor DNS. Alguien con malas intenciones podría, por

ejemplo, cambiar el archivo DNS para dirigirse a una dirección IP de fuera de la red. Podrían hacerse pasar por servidor de la red y, quizás, obtener acceso a información confidencial de los usuarios que visitaran el servidor.

Consideraciones de seguridad para utilizar el servidor HTTP paraiSeries

El servidor HTTP proporciona a los clientes navegadores de la World Wide Web el acceso a objetos multimedia del servidor iSeries, tales como documentos HTML (lenguaje de códigos hipertexto). También ofrece soporte para la especificación *Interfaz de pasarela común (CGI)*. Los programadores de aplicaciones pueden escribir programas CGI para ampliar la funcionalidad del servidor.

El administrador puede utilizar el Internet Connection Server o el servidor IBM HTTP para iSeries para ejecutar múltiples servidores a la vez en el mismo servidor iSeries. Cada servidor que está en ejecución se denomina una **instancia de servidor**. Cada instancia de servidor tiene un nombre exclusivo. El administrador controla qué instancias se inician, y qué puede hacer cada instancia.

Nota: Debe estar ejecutando la instancia *ADMIN en el servidor HTTP cuando utilice un navegador Web para configurar o administrar cualquiera de los elementos siguientes:

- Firewall para iSeries
- Internet Connection Server
- Internet Connection Secure Server
- IBM HTTP Server para iSeries

Un usuario (un visitante del sitio Web) nunca verá ninguna pantalla de Inicio de sesión de servidor iSeries. No obstante, el administrador del servidor iSeries debe autorizar explícitamente todos los documentos HTML y programas CGI, definiéndolos en directivas HTTP. Además, el administrador puede configurar tanto la seguridad de los recursos y la autenticación de los usuarios (ID de usuario y contraseña), en algunas o en todas las peticiones.

Un ataque por parte de un pirata podría dar como resultado la denegación de servicio al servidor Web. El servidor puede detectar un ataque de denegación de servicio midiendo el tiempo de espera de las peticiones de determinados clientes. Si el servidor no recibe una petición del cliente, el servidor determina que se está produciendo un ataque de denegación de servicio. Esto ocurre tras realizar la conexión inicial del cliente con el servidor. La acción por omisión del servidor es llevar a cabo la detección del ataque y la penalización.

Impedir el acceso a HTTP

Si *no* desea que nadie utilice el programa para acceder al sistema, deberá evitar la ejecución del servidor HTTP. Haga lo siguiente:

__ Paso 1. Para evitar que los trabajos del servidor HTTP se arranquen automáticamente al arrancar TCP/IP, teclee lo siguiente:

```
CHGHTTPA AUTOSTART(*NO)
```

Notas:

a. AUTOSTART(*NO) es el valor por omisión.

b. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

__ Paso 2. Por omisión, el trabajo del servidor HTTP utiliza el perfil de usuario QTMHHTTP. Para evitar que se arranque el servidor HTTP, establezca el estado del perfil de usuario QTMHHTTP en *DISABLED.

Control del acceso al servidor HTTP

El objetivo principal de ejecutar un servidor HTTP es proporcionar acceso a los visitantes a un sitio Web de su sistema iSeries. Piense en quienes visitan su sitio Web como las personas que leen un anuncio en un diario comercial. El visitante no está al corriente del hardware y el software que se ejecuta en el sitio Web, por ejemplo el tipo de servidor que está utilizando y dónde está ubicado físicamente el servidor. Por lo general, no deseará poner ninguna barrera (por ejemplo, una pantalla de inicio de sesión) entre un visitante potencial y el sitio Web. Sin embargo, quizá desee restringir el acceso a algunos documentos o programas de la CGI que se proporcionan en su sitio Web.

Quizá desee también que un solo sistema iSeries proporcione varios sitio Web lógicos.Por ejemplo, su sistema iSeries puede ofrecer soporte para sucursales diferentes de su empresa con conjuntos de clientes diferentes.Para cada una de estas sucursales de la empresa, desea que aparezca un solo sitio Web de modo totalmente independiente para el visitante. Además, quizá desee proporcionar sitios Web internos (una intranet) con información confidencial acerca de su empresa.

Como administrador de seguridad, debe asegurarse de proteger el contenido de su sitio Web y, al mismo tiempo, debe garantizar que sus prácticas de seguridad no afectan negativamente a su sitio Web. Además, debe asegurarse de que la actividad HTTP no arriesga la integridad del sistema o de la red. Los temas siguientes proporcionan sugerencias de seguridad cuando se utilice el programa.

Consideraciones sobre la administración

A continuación se citan algunas consideraciones sobre seguridad en la administración del servidor Internet.

- Puede realizar funciones de puesta a punto y de configuración utilizando un navegador Web y la instancia *ADMIN. Para algunas funciones, tales como crear instancias adicionales del servidor, *debe* utilizar el servidor *ADMIN.
- El URL por omisión para la página de inicio de administración (la página de inicio para el servidor *ADMIN) está publicado en la documentación de los productos que proporcionan funciones de administración de navegador. Por lo tanto, los piratas probablemente conocerán el URL por omisión y estará publicado en foros de piratas, al igual que se conocen y se publican las contraseñas por omisión de los perfiles por omisión proporcionados por IBM. Existen numerosas formas de protegerse de este riesgo:
  - Ejecutar solamente la instancia *ADMIN del servidor HTTP cuando necesite realizar funciones de administración. No tener la instancia *ADMIN en ejecución todo el tiempo.
  - Activar el soporte SSL para la instancia *ADMIN (utilizando el Gestor de Certificados Digitales). La instancia *ADMIN utiliza las directivas de protección HTTP para solicitar una contraseña y un ID de usuario. Al utilizar SSL, su ID de usuario y contraseña se cifran (junto con el resto de la información sobre la configuración que aparece en los formularios de administración).
  - Utilizar un cortafuegos para impedir el acceso al servidor *ADMIN desde Internet y para ocultar los nombres de dominio y de sistema, que forman parte del URL.

- Cuando lleve a cabo funciones de administración, debe iniciar la sesión con un perfil de usuario que tenga autorización especial *IOSYSCFG. Quizá también necesite autorización para especificar objetos en el sistema como, por ejemplo:
  - Las bibliotecas o los directorios que contienen documentos HTML y programas CGI.
  - Los perfiles de usuario que desee intercambiar entre las directivas para el servidor.
  - Las Listas de control de acceso (ACL) para todos los directorios que utilicen las directivas.
  - Un objeto de lista de validación para la creación y el mantenimiento de ID de usuario y contraseñas.

  Tanto con el servidor *ADMIN como con TELNET tiene la posibilidad de llevar a cabo funciones de administración de modo remoto, quizás a través de una conexión Internet. Si realiza la administración a través de un enlace público (Internet), puede exponer al husmeo una contraseña y un ID de usuario potentes. El ″husmeador″ puede utilizarlos para intentar acceder al sistema utilizando, por ejemplo, TELNET o FTP.

  Notas:

  1. Con TELNET, la pantalla de Inicio de sesión se trata como cualquier otra pantalla. Aunque la contraseña no se visualiza al teclearla, el sistema la transmite sin cifrado ni codificación.
  2. Con el servidor *ADMIN, la contraseña se codifica, pero no se cifra. El esquema de codificación es un estándar comercial y, por lo tanto, generalmente conocido entre la comunidad pirata. Aunque la codificación no resulta fácil de comprender para el ″pirata informático″ ocasional, un pirata informático con experiencia probablemente disponga de las herramientas necesarias para intentar decodificar la contraseña.

  Consejo de seguridad

  Si tiene pensado realizar la administración remota a través de Internet, deberá utilizar la instancia *ADMIN con SSL, de forma que las transmisiones estén cifradas. No utilice una aplicación poco segura, como una versión de TELNET anterior a la V4R4 (TELNET da soporte a SSL a partir de la V4R4). Si está utilizando el servidor *ADMIN a través de una intranet de usuarios *autorizados*, es probable que pueda utilizarlo con seguridad para la administración.

- Las directivas de HTTP proporcionan la base para todas las actividades en el servidor. La configuración entregada proporciona la posibilidad de ofrecer una página de Bienvenida por omisión. Un cliente no puede ver ninguno de los documentos del servidor excepto la página de Bienvenida hasta que el administrador del servidor define las directivas para el servidor. Para definir directivas, utilice un navegador Web y el servidor *ADMIN o el mandato Trabajar con configuración HTTP (WRKHTTPCFG). Ambos métodos requieren la autorización especial *IOSYSCFG. Al conectar el servidor iSeries a Internet, resulta aún más importante evaluar y controlar el número de usuarios de la organización que tienen autorización especial *IOSYSCFG.

Protección de los recursos

El servidor IBM HTTP para iSeries incluyen directivas HTTP que pueden proporcionar un control detallado de la información que utiliza el servidor. Puede utilizar las directivas para controlar desde qué directorios el servidor Web da

servicio a los URL para archivos HTML y programas CGI, para conmutar a otros perfiles de usuario y para requerir la autenticación de ciertos recursos.

Nota: La documentación de ″Web serving″ en Information Center proporciona descripciones completas de las directivas HTTP disponibles y cómo utilizarlas. A continuación se ofrecen algunas sugerencias y consideraciones para utilizar este soporte:

- El servidor HTTP empieza a partir de la base de ″autorización explícita″. El servidor no acepta una petición a menos que dicha petición esté definida explícitamente en las directivas. En otras palabras, el servidor rechaza inmediatamente todas las peticiones de un URL a menos que dicho URL esté definido en las directivas (por nombre o genéricamente).
- Puede utilizar directivas de protección para solicitar un ID de usuario y una contraseña antes de aceptar una petición de alguno de sus recursos o de todos ellos.
  - Cuando un usuario (cliente) solicita un recurso protegido, el servidor exige al navegador una contraseña y un ID de usuario. El navegador solicita al usuario que entre una contraseña y un ID de usuario y, a continuación, envía la información al servidor. Algunos navegadores almacenan la contraseña y el ID de usuario y los envían automáticamente con las peticiones siguientes. Esto exime al usuario de entrar repetidamente los mismos ID de usuario y contraseña en cada petición.

    Puesto que algunos navegadores almacenan la contraseña y el ID de usuario, hay que llevar a cabo la misma tarea de educación de usuario que se realiza cuando los usuarios entran en el sistema a través de la pantalla de Inicio de sesión del servidor iSeries o a través de un direccionador. Una sesión de navegador desatendida representa un riesgo de seguridad potencial.
  - Dispone de tres opciones relacionadas con el manejo de las contraseñas y de los ID de usuario por parte del sistema (especificadas en las directivas de protección):
    1. Puede utilizar la validación de perfiles de usuario y contraseñas normales del servidor iSeries. Por lo general, se utiliza para proteger los recursos de una intranet (red protegida).
    2. Puede crear ″usuarios de Internet″: usuarios que pueden validarse pero que no tienen un perfil de usuario en el servidor iSeries. Los usuarios de Internet se implementan mediante un objeto de servidor iSeries denominado ″lista de validación″. Los objetos de lista de validación contienen listas de usuarios y contraseñas definidos específicamente para su uso con una aplicación concreta.

       Puede decidir cómo se suministran los ID de usuario y las contraseñas de Internet (por ejemplo, mediante una aplicación o mediante un administrador como respuesta a una petición por correo electrónico), así como cómo gestionar los usuarios de Internet. Utilice la interfaz (con base en el navegador) del servidor HTTP para ponerlo a punto.

       Para las redes no seguras (Internet), el uso de usuarios de Internet proporciona una protección global mejor que el uso de perfiles de usuario y contraseñas normales. El conjunto exclusivo de los ID de usuario y contraseñas crea una limitación integrada respecto a lo que pueden hacer los usuarios. Las contraseñas y los ID de usuario no están disponibles en el inicio de sesión normal (por ejemplo, con TELNET o FTP). Además, no expone las contraseñas y los ID de usuario al husmeo.
    3. El protocolo LDAP (Lightweight directory access protocol) en un protocolo de servicios de directorio que proporciona acceso a un directorio a través

de un Protocolo de Control de Transmisión (TCP). Le permite almacenar información en ese servicio de directorio y consultarla. Ahora el LDAP está soportado como opción para la autenticación de usuario.

Notas:

1. Cuando el navegador envía el ID de usuario y la contraseña (ya sea para un perfil de usuario o para un usuario de Internet), están codificados, no cifrados. El esquema de codificación es un estándar comercial y, por lo tanto, generalmente conocido entre la comunidad pirata. Aunque la codificación no resulta fácil de comprender para el ″pirata informático″ ocasional, un pirata informático con experiencia probablemente disponga de las herramientas necesarias para intentar decodificarlos.
2. El servidor iSeries almacena el objeto de validación en un área protegida del sistema. Sólo puede acceder al mismo con las interfaces definidas del sistema (API) y la autorización adecuada.

– Puede utilizar el Gestor de certificados digitales (DCM) para crear su propia Autoridad certificadora en la intranet. El Certificado digital asocia automáticamente un certificado con el perfil de usuario del propietario. El certificado tiene las mismas autorizaciones y los mismos permisos que el perfil asociado.

- Cuando el servidor acepta una petición, entra en función la seguridad normal de los recursos del servidor iSeries. El perfil de usuario que ha solicitado el recurso debe disponer de la autorización necesaria para el recurso (por ejemplo, la carpeta o el archivo físico del recurso que contiene el documento HTML). Por omisión, los trabajos se ejecutan bajo el perfil de usuario QTMHHTTP. Puede utilizar una directiva para cambiar a un perfil de usuario distinto. En este caso, el sistema utiliza la autorización del perfil de usuario para acceder a los objetos. A continuación se ofrecen algunas consideraciones para este soporte:
  – El intercambio de perfiles de usuario puede resultar especialmente útil cuando el servidor proporciona más de un sitio Web lógico. Puede asociar un perfil de usuario diferente a las directivas para cada sitio Web y utilizar la seguridad normal de recursos del servidor iSeries para proteger los documentos de cada sitio.
  – Puede utilizar la posibilidad de intercambiar perfiles de usuario en combinación con el objeto de validación. El servidor utiliza un ID de usuario y una contraseña exclusivos (separados del ID de usuario y contraseña normales) para evaluar la petición inicial. Una vez el servidor ha autenticado al usuario, el sistema cambia a un perfil de usuario diferente, beneficiándose de la seguridad de los recursos del. Así, el usuario no conoce el nombre verdadero del perfil de usuario y no puede intentar utilizarlo de otros modos (tales como FTP).
- Algunas peticiones del servidor HTTP necesitan ejecutar un programa en el servidor HTTP. Por ejemplo, un programa podría acceder a datos de su sistema. Para que el programa pueda ejecutarse, el administrador del sistema debe correlacionar la petición (URL) con un programa específico definido por el usuario, que se ajuste a los estándares de interfaz de usuario CGI. A continuación, se incluyen algunas consideraciones para los programas CGI:
  – Puede utilizar las directivas de protección para los programas CGI tal y como lo hace para documentos HTML. Así, puede solicitar una contraseña y un ID de usuario antes de ejecutar el programa.
  – Por omisión, los programas CGI se ejecutan bajo el perfil de usuario QTMHHTP1. Puede cambiar a un perfil de usuario diferente antes de ejecutar

el programa. Por consiguiente, puede establecer la seguridad normal de recursos del servidor iSeries para los recursos a los que acceden los programas CGI.

– Como administrador de seguridad, debe revisar la seguridad antes de autorizar la utilización de cualquier programa CGI en el sistema. Debe conocer la procedencia del programa y las funciones que realiza el programa CGI. También debe supervisar las posibilidades de los perfiles de usuario bajo los cuales está ejecutando los programas CGI y efectuar una comprobación con los programas CGI para determinar, por ejemplo, si puede acceder a una línea de mandatos. Trate los programas CGI con la misma vigilancia con la que trata los programas que adoptan la autorización.

– Asimismo, debe asegurarse de evaluar los objetos confidenciales que pueden tener una autorización de uso público inadecuada. En algunas ocasiones, un programa CGI no diseñado correctamente, permite que un usuario engañoso y con los conocimientos necesarios intente vagar por el sistema.

– Utilice una biblioteca de usuario específica, por ejemplo, la CGILIB, para mantener todos los programas de CGI. Utilice la autorización sobre objetos para controlar quién puede colocar nuevos objetos en esa biblioteca y quién puede ejecutar programas en ella. Utilice las directivas para limitar el servidor HTTP a ejecutar programas de CGI que estén en esa biblioteca.

Nota: Si el servidor proporciona varios sitios Web lógicos, quizá desee establecer una biblioteca para los programas CGI de cada sitio.

Otras consideraciones sobre la seguridad

A continuación se describen otras consideraciones sobre la seguridad:

- HTTP proporciona acceso de sólo lectura al sistema iSeries.Las peticiones del servidor HTTP no pueden actualizar ni suprimir datos directamente del sistema. No obstante, puede tener programas CGI que actualicen datos. Además, puede habilitar el programa CGI Net.Data para acceder a la base de datos del iSeries. El sistema utiliza un script (que es similar a un programa de salida) para evaluar las peticiones para el programa Net.Data. Por consiguiente, el administrador del sistema puede controlar las acciones que puede llevar a cabo el programa Net.Data.
- El servidor HTTP proporciona unas anotaciones cronológicas de acceso que puede utilizar para supervisar los accesos y los intentos de acceso a través del servidor.

Consideraciones de seguridad para utilizar SSL con el servidorIBM HTTP para iSeries

El servidor IBM HTTP para iSeries puede proporciona conexiones seguras con la Web para el servidor iSeries. Un **sitio web seguro** indica que las transmisiones entre el cliente y el servidor están cifradas (en ambas direcciones). Estas transmisiones cifradas están protegidas frente a los husmeadores y los que intentan capturar o modificar las transmisiones.

Nota: Recuerde que el sitio Web seguro se aplica estrictamente a la seguridad de la información que pasa entre el cliente y el servidor. Su finalidad no es la de reducir la vulnerabilidad del servidor ante los piratas informáticos. No obstante, sí limita la información que podría obtener fácilmente un supuesto pirata que se dedicara a husmear.

Los temas sobre SSL y servidores Web (HTTP) del Information center proporcionan información completa para instalar, configurar y gestionar el proceso de cifrado.

Estos temas proporcionan tanto una visión general de las características del servidor como algunas consideraciones para su utilización.

Internet Connection Server proporciona soporte HTTP y HTTPS cuando se instala uno de los siguientes programas bajo licencia:

- 5722–NC1
- 5722–NCE

Cuando están instaladas estas opciones, se hace referencia al producto como Internet Connection Secure Server.

El servidor IBM HTTP para iSeries (5722–DG1) proporciona soporte de http y https. Debe instalar uno de los siguientes productos criptográficos para habilitar SSL:

- 5722–AC2
- 5722–AC3

La seguridad que depende del cifrado tiene numerosos requisitos:

- Tanto el remitente como el receptor (servidor y cliente) deben ″comprender″ los mecanismos de cifrado y poder llevar a cabo el cifrado y el descifrado. El servidor HTTP requiere un cliente con SSL habilitado. (Los navegadores Web más utilizados tienen SSL habilitado). Los programas bajo licencia de cifrado de iSeries ofrecen soporte para numerosos métodos de cifrado estándar del mercado.Cuando un cliente intenta establecer una sesión segura, el servidor y el cliente negocian para localizar el método de cifrado más seguro para el que ambos ofrezcan soporte.
- Un escuchador oculto no debe poder descifrar la transmisión. Así, los métodos de cifrado requieren que ambas partes dispongan de una **clave privada** de cifrado y de descifrado que sólo conozcan ellos. Si desea tener un sitio Web *externo* seguro, debería utilizar una autoridad certificadora (CA) independiente para crear y emitir certificados digitales a los usuarios y servidores. A la autoridad certificadora se la denomina interlocutor de confianza.

El cifrado protege la confidencialidad de la información transmitida. Sin embargo, para la información confidencial, por ejemplo, información económica, además de la confidencialidad, también se precisa la integridad y la autenticidad. En otras palabras, el cliente y (opcionalmente) el servidor deben autorizar a la otra parte (a través de una consulta independiente) y asegurarse de que la transmisión no se ha alterado. La firma digital que proporcionan las autoridades certificadoras (CA) proporcionan estos seguros de autenticidad e integridad. El protocolo SSL proporciona autenticación mediante la verificación de la firma digital del certificado del servidor (y, opcionalmente, del certificado del cliente).

El cifrado y el descifrado requieren tiempo de proceso, que influye en el rendimiento de las trasmisiones. Por consiguiente, los servidores iSeries proporcionan la posibilidad de ejecutar los programas para el servicio seguro y no seguro al mismo tiempo. Puede utilizar el servidor HTTP no seguro para ofrecer documentos que no requieran seguridad, por ejemplo, el catálogo de productos. Estos documentos dispondrán de un URL que se inicie con `http://` . Puede utilizar un servidor HTTP seguro para la información delicada, por ejemplo el formulario en el que el cliente incluye la información de su tarjeta de crédito. El programa puede atender a documentos cuyo URL empiece con `http://` o con `https://`.

Recordatorio

Es buena práctica de Internet (netiquette) informar a sus clientes cuándo son seguras las transmisiones y cuándo no, especialmente cuando su sitio Web utilice solamente un servidor seguro en ciertos documentos.

Recuerde que el cifrado requiere un cliente y un servidor seguros. Los navegadores seguros (clientes HTTP) son cada vez más habituales.

Consideraciones de seguridad para LDAP

Las características de seguridad de LDAP (Lightweight Directory Access Protocol) incluyen Capa de Sockets Segura (SSL), Listas de control de acceso y cifrado de contraseñas CRAM-MD5. En la V5R1 también se han añadido las conexiones Kerberos y el soporte de Auditoría de seguridad para mejorar la seguridad de LDAP.

Para obtener más información sobre estos temas, consulte iSeries Information Center—>Redes–>TCP/IP–>Servicios de directorio (LDAP). Consulte "Requisitos e información relacionada" en la página xii para obtener información sobre cómo acceder a iSeries Information Center.

Consideraciones de seguridad para LPD

El LPD (daemon de impresora de líneas) proporciona la posibilidad de distribuir la salida de impresora para el sistema. El sistema no realiza ningún proceso de inicio de sesión para LPD.

Impedir el acceso a LPD

Si *no* quiere que nadie utilice LPD para acceder al sistema, debe evitar que funcione el servidor LPD. Haga lo siguiente:

__ Paso 1. Para evitar que los trabajos del servidor LPD se arranquen automáticamente al arrancar TCP/IP, teclee lo siguiente:

```
CHGLPDA AUTOSTART(*NO)
```

Notas:

a. AUTOSTART(*YES) es el valor por omisión.

b. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

__ Paso 2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para LPD, haga lo siguiente:

__ Paso a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.

__ Paso b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).

__ Paso c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).

__ Paso d. Para el rango del puerto más bajo, especifique `515`.

__ Paso e. Para el rango del puerto más alto, especifique `*ONLY`.

Notas:

1) La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.
2) RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

__ Paso f. Para el protocolo, especifique `*TCP`.

__ Paso g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.

__ Paso h. Repita los pasos del 2c al 2g para el protocolo *UDP.

Control del acceso a LPD

Si quiere permitir a los clientes de LPD que accedan al sistema tenga en cuenta los elementos de seguridad siguientes:

- Para evitar que un usuario llene el sistema con objetos no deseados, asegúrese de establecer límites de umbral adecuados para las agrupaciones de almacenamiento auxiliar (ASP). Puede visualizar y establecer los umbrales para las ASP utilizando las herramientas de servicio del sistema (SST) o las herramientas de servicio dedicado (DST). La publicación *Copia de seguridad y recuperación* proporciona más información acerca de los umbrales de ASP.
- Puede utilizar la autorización sobre las colas de salida para restringir quién puede enviar archivos en spool al sistema. Los usuarios de LPD sin un ID de usuario utilizan el perfil de usuario QTMPLPD. Puede dar acceso a este perfil de usuario únicamente a unas pocas colas de salida.

Consideraciones de seguridad para SNMP

El servidor iSeries puede actuar como un agente del Protocolo simple de gestión de red (SNMP) en una red. El SNMP proporciona un medio para gestionar las pasarelas, direccionadores y sistemas principales de un entorno de red. Un agente SNMP recoge información acerca del sistema y realiza las funciones que solicitan los gestores remotos de la red SNMP.

Impedir el acceso a SNMP

Si *no* quiere que nadie utilice SNMP para acceder al sistema, debe evitar el funcionamiento del servidor SNMP. Haga lo siguiente:

__ Paso 1. Para evitar que los trabajos servidores SNMP se arranquen automáticamente al arrancar TCP/IP, teclee lo siguiente:

```
CHGSNMPA AUTOSTART(*NO)
```

Notas:

a. AUTOSTART(*YES) es el valor por omisión.
b. "Control de los servidores TCP/IP que se inician automáticamente" en la página 132 proporciona más información acerca del control de los servidores TCP/IP que se inician automáticamente.

__ Paso 2. Para evitar que alguien asocie una aplicación de usuario, tal como una aplicación socket, con el puerto que el sistema utiliza normalmente para SNMP, haga lo siguiente:

__ Paso a. Teclee `GO CFGTCP` para visualizar el menú Configurar TCP/IP.

__ Paso b. Seleccione la opción 4 (Trabajar con restricciones de puerto TCP/IP).

__ Paso c. En la pantalla Trabajar con restricciones de puerto TCP/IP, especifique la opción 1 (Añadir).

__ Paso d. Para el rango del puerto más bajo, especifique `161`.

__ Paso e. Para el rango del puerto más alto, especifique `*ONLY`.

Notas:

1) La restricción de puertos entra en vigor cuando se vuelve a arrancar TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puertos, debe finalizar TCP/IP y arrancarlo de nuevo.
2) RFC1700 proporciona información sobre las asignaciones de números de puerto comunes.

__ Paso f. Para el protocolo, especifique `*TCP`.

__ Paso g. Para el campo de perfil de usuario, especifique un nombre de perfil de usuario protegido en el sistema. (Los perfiles de usuario protegidos no son propietarios de programas que adoptan autorización y no tienen contraseñas conocidas por otros usuarios.) Restringiendo el puerto a un usuario específico, excluye automáticamente a todos los demás usuarios.

__ Paso h. Repita los pasos del 2c al 2g para el protocolo *UDP.

Control del acceso a SNMP

Si quiere permitir que los gestores de SNMP accedan al sistema tenga en cuenta los elementos de seguridad siguientes:

- Alguien que pueda acceder a la red con SNMP puede reunir información acerca de la red. La información que ha ocultado utilizando seudónimos y un servidor de nombres de dominio está disponible para el supuesto intruso a través de SNMP. Además, un intruso puede utilizar SNMP para modificar la configuración de la red y destruir las comunicaciones.
- SNMP confía en un nombre de comunidad para el acceso. En teoría, el nombre de comunidad es similar a una contraseña. El nombre de comunidad no está cifrado. Por consiguiente, es vulnerable al husmeo. Utilice el mandato Añadir comunidad para SNMP (ADDCOMSNMP) para establecer el parámetro de dirección Internet del gestor (INTNETADR) como una o varias direcciones IP específicas en lugar de *ANY. También puede establecer el parámetro OBJACC de los mandatos ADDCOMSNMP o CHGCOMSNMP en *NONE, para evitar que los gestores de una comunidad accedan a objetos MIB. Esto está pensado para hacerse sólo temporalmente, para denegar el acceso a los gestores de una comunidad sin eliminar la comunidad.

Consideraciones de seguridad para el servidor INETD

Al contrario que la mayoría de los servidores TCP/IP, el servidor INETD no proporciona un único servicio a los clientes, sino que proporciona servicios varios que los administradores pueden personalizar. Por ese motivo, al servidor INETD se le conoce a veces como ″el superservidor″. El servidor INETD tiene incorporados los siguientes servicios:

- time
- daytime
- echo
- discard
- changed

Estos servicios están soportados para TCP y para UDP. Para UDP, los servicios echo, time, daytime y changed reciben paquetes UDP y, a continuación devuelven los paquetes al originador. El servidor echo server devuelve los paquetes que recibe, los servidores time y daytime generan la hora en un formato específico y lo devuelven y el servidor changed genera un paquete de caracteres ASCII imprimibles y lo devuelven.

La naturaleza de estos servicios UDP hace al sistema vulnerable a ataques de denegación de servicio. Por ejemplo, supongamos que tiene dos servidores iSeries: SYSTEMA y SYSTEMB. Un programador malintencionado podría falsificar la cabecera IP y la cabecera UDP con una dirección de origen de SYSTEMA y un número de puerto UDP del servidor time. Entonces podría enviar ese paquete al servidor time en el SYSTEMB, que enviará la hora al SYSTEMA, que volverá a responder al SYSTEMB, y así sucesivamente, generando un bucle continuo y consumiendo recursos de CPU en ambos sistemas, así como el ancho de banda de la red.

Por consiguiente, deberá tener en cuenta el riesgo de un ataque de este tipo en su sistema iSeries y ejecutar estos servicios solamente en una red segura. El servidor INETD se envía definido para que no se inicie automáticamente al iniciar TCP/IP. Puede configurar si se iniciarán los servicios o no al iniciarse INETD. Por omisión, los servidores time y daytime de TCP y UDP se inician al iniciar el servidor INETD.

Existen dos archivos de configuración para el servidor INETD:

```
/QIBM/UserData/OS400/inetd/inetd.conf
/QIBM/ProdData/OS400/inetd/inetd.conf
```

Estos archivos determinan qué programas deben iniciarse cuando se inicia el servidor INETD. También determinan bajo qué perfil de usuario se ejecutan estos programas cuando INETD los inicias.

Nota: El archivo de configuración en proddata no debe modificarse nunca. Se sustituye cada vez que vuelve a cargarse el sistema. Los cambios en la configuración de clientes sólo deberán colocarse en el archivo del árbol de de directorios userdata, ya que dicho archivo **no** se actualiza durante las actualizaciones de release.

Si un programador malintencionado accediera a estos archivos, podría configurarlos para iniciar cualquier programa al iniciarse INETD. Por consiguiente,

es de suma importancia proteger estos archivos. Para realizar cambios en ellos, requieren por omisión la autorización QSECOFR. No debe reducir la autorización necesaria para acceder a ellos.

Nota: No modifique el archivo de configuración del directorio ProdData. Ese archivo se sustituye cada vez que se vuelve a cargar el sistema. Los cambios en la configuración de clientes sólo deberán colocarse en el archivo del árbol de directorios UserData, ya que dicho archivo no se actualiza durante las actualizaciones de release.

Consideraciones de seguridad para limitar TCP/IP itinerante

Si el sistema está conectado a una red, querrá limitar las posibilidades del usuario para vagar por la red con las aplicaciones TCP/IP. Una forma de hacerlo es restringir el acceso a los siguientes mandatos TCP/IP de cliente:

Nota: Estos mandatos pueden existir en numerosas bibliotecas del sistema. Se encuentran tanto en la biblioteca QSYS como en la biblioteca QTCP, como mínimo. Asegúrese de localizar y asegurar todas las ocurrencias.

- STRTCPFTP
- FTP
- STRTCPTELN
- TELNET
- LPR
- SNDTCPSPLF
- RUNRMTCMD (cliente REXEC)

Los posibles destinos del usuario están determinados por lo siguiente:

- Entradas en la tabla del sistema principal TCP/IP.
- La entrada *DFTROUTE en la tabla de ruta TCP/IP. Esto permite a los usuarios entrar la dirección IP del sistema del salto siguiente cuando su destino es una red desconocida. Un usuario puede alcanzar o poner en contacto una red remota utilizando la ruta por omisión.
- Configuración del servidor de nombre remoto. Este soporte permite a otro servidor de la red ubicar nombres de sistemas principales para los usuarios.
- Tabla del sistema remoto.

Necesita controlar quién puede añadir entradas a estas tablas y cambiar la configuración. También necesita entender las implicaciones de sus entradas de tabla y de su configuración.

Tenga en cuenta que un usuario experimentado con acceso a un compilador ILE C puede crear un programa socket que se conecte a un puerto TCP o UDP. Puede dificultar esta operación restringiendo el acceso a los archivos de interfaz de socket de la biblioteca QSYSINC:

- SYS
- NETINET
- H
- ARPA
- sockets y SSL

En los programas de servicio, se puede restringir el uso de sockets y aplicaciones SSL que ya estén compiladas, restringiendo el uso de los siguientes programas de servicio:

- QSOSRV1

- QSOSRV2
- QSOSKIT(SSL)
- QSOSSLSR(SSL)

Los programas de servicio se entregan con autorización de uso público *USE, aunque la autorización se puede cambiar por *EXCLUDE (u otro valor).

Capítulo 14. Acceso seguro a estaciones de trabajo

Muchos usuarios del sistema tienen un PC en la mesa como estación de trabajo. Utilizan herramientas que funcionan en el PC y utilizan el PC para conectarse al servidor iSeries.

La mayoría de los métodos de conexión de un PC a servidores iSeries proporcionan más funcionalidad que la emulación de estación de trabajo. El PC puede parecer una pantalla de iSeries y proporcionar al usuario sesiones de inicio de sesión interactivas. Además, el PC puede parecer otro sistema para los servidores iSeries y proporcionar funciones tales como transferencia de archivos y llamada de procedimiento remoto.

Como administrador de seguridad de un servidor iSeries, necesita tener en cuenta lo siguiente:

- las funciones disponibles para los usuarios de PC que están conectados al sistema,
- los recursos del servidor iSeries a los que pueden acceder los usuarios de PC.

Querrá evitar funciones avanzadas de PC (tales como transferencia de archivos y llamada de procedimiento remoto), si el esquema de seguridad del servidor iSeries no está preparado todavía para tales funciones. Probablemente el objetivo a largo plazo sea permitir las funciones avanzadas de PC mientras se protege la información del sistema. En los temas siguientes se tratan ciertos elementos de seguridad asociados al acceso de PC.

Prevención de virus en las estaciones de trabajo

Esta información sugiere métodos para que los administradores de seguridad puedan proteger los PC ante los virus.

Protección del acceso a datos de estación de trabajo

Parte del software de cliente PC utiliza carpetas compartidas para almacenar información en el servidor. Para acceder a los archivos de la base de datos del iSeries, el usuario de PC tiene un conjunto limitado, bien definido de interfaces. Con la posibilidad de transferencia de archivos que forma parte de la mayoría del software cliente/servidor, el usuario de PC puede copiar archivos entre el servidor y el PC. Con la posibilidad de acceso a base de datos, tal como un archivo DDM, SQL remoto, o un controlador ODBC, el usuario de PC puede acceder a los datos del servidor.

En este entorno puede crear programas para interceptar y evaluar peticiones de usuario de PC para acceder a los recursos del servidor. Cuando las peticiones utilizan un archivo DDM, especifique el programa de salida en el atributo de red Acceso a la gestión de datos distribuidos (DDMACC). Para algunos métodos de transferencia de archivos de PC se especifica el programa de salida en el atributo de red Acceso de petición de cliente (PCSACC). O bien puede especificar PCSACC(*REGFAC) para utilizar la función de registro. Cuando las peticiones utilizan otras funciones del servidor para acceder a los datos, puede utilizar el mandato WRKREGINF para registrar los programas de salida para tales funciones del servidor.

Los programas de salida, sin embargo, pueden ser difíciles de diseñar y en raras ocasiones son infalibles. Los programas de salida no son una sustitución de la autorización de objetos, que está diseñada para proteger los objetos del acceso no autorizado de cualquier fuente.

Parte del software de cliente, por ejemplo IBM iSeries Access para Windows, utiliza el sistema de archivos integrado para almacenar y acceder a los datos de servidores iSeries. Con el sistema de archivos integrado, todo el servidor resulta más fácilmente disponible para los usuarios de PC. La autorización sobre objetos se vuelve incluso más importante. A través del sistema de archivos integrado, un usuario con la autorización suficiente puede ver una biblioteca de servidor como si fuera un directorio de PC. Mediante mandatos simples de mover y copiar se pueden mover datos instantáneamente de una biblioteca del servidor iSeries a un directorio de PC o viceversa. El sistema hace automáticamente los cambios adecuados en el formato de los datos.

Notas:

1. Puede utilizar una lista de autorizaciones para controlar la utilización de objetos en el sistema de archivos QSYS.LIB. Consulte el apartado "Restricción del acceso al sistema de archivos QSYS.LIB" en la página 110 para obtener más información.
2. En el Capítulo 11, "Utilización del Sistema de Archivos Integrado (IFS) para proteger archivos", en la página 103 se proporciona más información acerca de los temas de seguridad con el sistema de archivos integrado.

La fortaleza del sistema de archivos integrado es su simplicidad para usuarios y programadores. Con una sola interfaz, el usuario puede trabajar con objetos en varios entornos. El usuario de PC no necesita software o API especiales para acceder a los objetos. En lugar de eso, el usuario de PC puede utilizar mandatos de PC conocidos o "seleccionar y pulsar" para trabajar directamente con los objetos.

Para todos los sistemas que tengan PC conectados, pero especialmente para los sistemas con software de cliente que utilice el sistema de archivos integrado, resulta decisivo un buen esquema de autorización sobre objetos. Debido a que la seguridad está integrada en el producto OS/400, cualquier petición para acceder a los datos debe pasar a través del proceso de comprobación de autorización. La comprobación de autorización se aplica a las peticiones de cualquier fuente y para el acceso a datos que utilicen cualquier método.

Autorización sobre objetos con acceso desde estación de trabajo

Al configurar la autorización sobre objetos, es necesario evaluar lo que la autorización proporciona al usuario de PC. Por ejemplo, cuando un usuario tiene autorización *USE sobre un archivo, el usuario puede ver o imprimir datos en el archivo. El usuario no puede cambiar la información del archivo ni suprimirlo. Para el usuario de PC, ver es equivalente a "leer", lo cual proporciona al usuario autorización suficiente para hacer una copia de un archivo en el PC. Este no será probablemente el objetivo pretendido.

En el caso de algunos archivos de gran importancia, necesitará establecer la autorización de uso público en *EXCLUDE para evitar que los copien en el PC. Puede proporcionar entonces otro método para "ver" el archivo en el servidor, tal como utilizar un menú y programas que adopten la autorización.

Otra opción para evitar la copia de archivos es utilizar un programa de salida que se ejecute siempre que un usuario de PC inicie una función del servidor (que no sea el inicio de sesión interactivo). Puede especificar un programa de salida en el atributo de red PCSACC utilizando el mandato Cambiar atributo de red (CHGNETA). O puede registrar programas de salida utilizando el mandato Trabajar con información de registro (WRKREGINF). El método que utilice dependerá del modo en que los PC accedan a los datos del sistema y del programa cliente que utilicen los PC. El programa de salida (QIBM_QPWFS_FILE_SERV) es aplicable al acceso IFS de iSeries Access y Net Server. No impide el acceso desde un PC con otros mecanismos, como FTP u ODBC.

Normalmente, el software del PC proporciona la posibilidad de subir, de forma que un usuario pueda copiar datos de un PC a un archivo de base de datos del servidor. Si no ha configurado correctamente el esquema de autorizaciones, un usuario de PC puede recubrir todos los datos de un archivo con datos desde un PC. Debe asignar la autorización *CHANGE cuidadosamente. Revise el Apéndice D de la publicación *iSeries Security Reference* para comprender la autorización necesaria para operaciones de archivo.

El iSeries Information Center proporciona más información sobre la autorización para las funciones de PC y sobre la utilización de programas de salida. Vea "Requisitos e información relacionada" en la página xii para obtener más detalles.

Administración de aplicaciones

La Administración de aplicaciones es un componente instalable opcionalmente de iSeries Navigator, la interfaz gráfica de usuario (GUI) para el servidor iSeries. La Administración de aplicaciones permite a los administradores del sistema controlar las funciones o las aplicaciones disponibles para otros usuarios y grupos en un servidor específico. Esto incluye el control de las funciones disponibles para los usuarios que acceden a sus servidores a través de clientes. Es importante destacar aquí que, si accede al servidor desde un cliente Windows, será el usuario del servidor iSeries y no el usuario de Windows el que determine qué funciones están disponibles para la administración.

Para obtener una documentación completa sobre la Administración de Aplicaciones de iSeries Navigator, consulte iSeries Information Center–>Conexión a iSeries—>Con qué conectarse —>iSeries Navigator (../html/as400/v5r2/ic2924/info/rzaj3/rzaj3overview.htm).

Administración de políticas

Las políticas son una herramienta para que la utilicen los administradores al configurar software en sus PC cliente. Las políticas pueden restringir las funciones y aplicaciones a las que puede acceder un usuario en el PC. Las políticas también pueden sugerir o imponer configuraciones para que las utilicen determinados usuarios o determinados PC.

Nota: Las políticas no ofrecen control sobre los recursos del servidor. Las políticas no son un sustituto de la seguridad del servidor. Las políticas pueden utilizarse para afectar a la forma en que iSeries Access accede al servidor desde un PC concreto, por parte de un usuario concreto. No obstante, no cambian la manera en que se accede a los recursos del servidor a través de otros mecanismos.

Las políticas se almacenan en un servidor de archivos. Cada vez que el usuario inicia la sesión en la estación de trabajo Windows, las políticas aplicables a ese

usuario de Windows se bajan desde el servidor de archivos. Las políticas se aplican al registro antes de que el usuario lleve a cabo acción alguna en la estación de trabajo.

Las políticas de Microsoft frente a la administración de aplicaciones

iSeries Access Express soporta dos estrategias distintas para implementar el control de administración dentro de su red: las políticas del sistema Microsoft y la Administración de Aplicaciones de iSeries Navigator. Tenga en cuenta lo siguiente al decidir qué estrategia se ajusta mejor a sus necesidades.

Políticas del sistema Microsoft

Las políticas son reguladas por el PC, no dependen de los releases específicos del OS/400. Las políticas pueden ser aplicables a los PC, así como a los usuarios de Windows. Esto significa que los usuarios se refieren al perfil de usuario de Windows, no al perfil de usuario del servidor. Las políticas pueden utilizarse para "configurar", así como para restringir. Por lo general, las políticas pueden ofrecer más granularidad que la Administración de aplicaciones y pueden ofrecen un mayor rango de funciones. Esto se debe a que no es necesaria la conexión con el servidor para determinar si el usuario puede utilizar o no la función. La implementación de políticas es más complicada que la implementación de la Administración de aplicaciones debido a que es necesario el uso del editor de políticas del sistema Microsoft y los PC deben configurarse individualmente para bajar las políticas.

Administración de aplicaciones de iSeries Navigator

La Administración de aplicaciones asocia datos con el perfil de usuario, en lugar del perfil de Windows con el que se asocian las políticas del sistema Microsoft. Aunque es necesario que los servidores iSeries ejecuten la V4R3 o una versión posterior del producto OS/400 para poder utilizar la Administración de aplicaciones, algunas funciones solamente están disponibles en la V4R4 o posteriores. La Administración de aplicaciones utiliza la interfaz gráfica de usuario de iSeries Navigator para administrar, lo que resulta más fácil que utilizar el editor de políticas. La información de la Administración de aplicaciones se aplica al usuario, independientemente del PC desde el que se conecte. Pueden restringirse funciones concretas de iSeries Navigator. La Administración de aplicaciones es preferible si todas las funciones que desea restringir están habilitadas para la Administración de aplicaciones y si la versión de OS/400 que se utiliza soporta la Administración de aplicaciones.

Utilización de SSL con iSeries Access para Windows

Para obtener información sobre el uso de iSeries Access Express con SSL, revise los temas del iSeries Information Center *Administración de la capa de sockets segura (SSL), Protección de iSeries Access Express e iSeries Navigator, iSeries Developer Kit para Java e iSeries Java Toolbox*, bajo el tema principal Java. También puede revisar esta información en el CD suministrado con el sistema.

Seguridad de iSeries Navigator

iSeries Navigator proporciona una interfaz fácil de utilizar con el servidor para los usuarios que tienen iSeries Access. Con cada release nuevo del producto OS/400, es posible acceder a más funciones del servidor a través de iSeries Navigator. Una

interfaz de fácil manejo proporciona muchas ventajas, lo que incluye un coste bajo de soporte técnico y una imagen mejorada para el sistema. También supone retos en la seguridad.

Como administrador de seguridad ya no puede confiar en la ignorancia de los usuarios para proteger los recursos. iSeries Navigator convierte muchas funciones en funciones sencillas y visibles para los usuarios. Debe asegurarse de diseñar e implementar políticas de seguridad para los perfiles de usuario y la seguridad de objetos para cumplir las necesidades de seguridad.

La V4R4 y versiones posteriores de IBM e(logo)server iSeries Access para Windows proporcionan los siguientes métodos para controlar las funciones que los usuarios pueden realizar mediante iSeries Navigator:

- Instalación selectiva
- Administración de aplicaciones
- Soporte de política del sistema Windows NT

El iSeries Navigator viene empaquetado como múltiples componentes que puede instalar por separado. Ello le permitirá instalar sólo las funciones que necesite. La Administración de aplicaciones permite a los administradores controlar las funciones a las que un usuario o un grupo pueden acceder mediante iSeries Navigator. La administración de aplicaciones organiza las aplicaciones en las siguientes categorías:

iSeries Navigator
Incluye iSeries Navigator y conectores adicionales.

Aplicaciones de cliente
Incluye todas las demás aplicaciones de cliente, incluyendo iSeries Access, que porporcionan funciones en los clientes administrados mediante la Administración de Aplicaciones.

Aplicaciones de sistema principal
Incluye todas las aplicaciones que residen por completo en el servidor y que proporcionan funciones administradas mediante la Administración de aplicaciones.

Puede utilizar la instalación selectiva, administración de aplicaciones y políticas para limitar las funciones de iSeries a las que podrá acceder un usuario. Ninguna de ellas, no obstante, debe utilizarse para la seguridad por recursos.

A partir de la V4R4, IBM e(logo)server iSeries Access para Windows también soporta el uso del Editor de políticas del sistema de Windows NT para controlar qué funciones pueden llevarse a cabo desde un cliente PC concreto, sin tener en cuenta quién esté utilizando ese PC.

Consulte el iSeries Information Center para obtener información adicional sobre la instalación selectiva, la Administración de aplicaciones y la Administración de políticas. El apartado “Acceso limitado a las funciones del programa” en la página 5 de este manual también trata la administración de aplicaciones.

Impedir el acceso a ODBC

Conectividad de base de datos abierta (ODBC) es una herramienta que pueden utilizar las aplicaciones de PC para acceder a los datos del iSeries como si fueran datos de PC. El programador de ODBC puede hacer que la ubicación física de los datos sea transparente al usuario de la aplicación del PC. Para obtener más

información sobre las consideraciones de seguridad de ODBC, vaya a la información de ″iSeries Access para Windows Seguridad de ODBC″ (/rzaii/rzaiiodbc09.HTM), ubicada en iSeries Information Center.

Consideraciones de seguridad para contraseñas de sesión de estación de trabajo

Normalmente, cuando un usuario de PC arranca el software de conexión, como iSeries Access, el usuario teclea una vez el ID de usuario y la contraseña del servidor. La contraseña se cifra y se almacena en la memoria del PC. Siempre que el usuario establezca una nueva sesión con el mismo servidor, el PC envía automáticamente el ID de usuario y la contraseña.

Parte del software de cliente/servidor proporciona también la opción de ignorar la pantalla de inicio de sesión para sesiones interactivas. El software enviará el ID de usuario y la contraseña cifrada cuando el usuario arranque una sesión interactiva (emulación 5250). Para soportar esta opción, el valor del sistema QRMTSIGN del servidor debe establecerse en *VERIFY.

Cuando se elige permitir que se ignore la pantalla Inicio de sesión, debe tener en cuenta las contrapartidas en la seguridad.

Riesgo de seguridad: Para la emulación 5250 o cualquier otro tipo de sesión interactiva, la pantalla Inicio de sesión es la misma que cualquier otra pantalla. A pesar de que cuando se teclea la contraseña no se visualiza en la pantalla, la contraseña se envía a través del enlace sin cifrar igual que cualquier otro campo de datos. Para algunos tipos de enlace, esto puede proporcionar a un futuro intruso la oportunidad de supervisar el enlace y detectar un ID de usuario y una contraseña. La supervisión de un enlace utilizando equipo electrónico se denomina a menudo **rastreo**. A partir de la V4R4, puede utilizar la capa de sockets segura (SSL) para cifrar las comunicaciones entre iSeries Access y el servidor iSeries. Así se protegen los datos, incluidas las contraseñas, contra el husmeo.

Cuando se elige la opción de ignorar la pantalla Inicio de sesión, el PC cifra la contraseña antes de enviarla. El cifrado evita la posibilidad de que se robe una contraseña mediante la técnica del rastreo. Sin embargo, debe asegurarse de que los usuarios de PC practiquen la seguridad operativa. Un PC no atendido con una sesión activa en el sistema iSeries proporciona la oportunidad de arrancar otra sesión sin conocer un ID de usuario y una contraseña.Los PC deben estar preparados para bloquearse cuando el sistema permanece inactivo durante un período prolongado, y deben requerir una contraseña para reanudar la sesión.

Aunque no se elija ignorar la pantalla Inicio de sesión, un PC no atendido con una sesión activa representa un riesgo para la seguridad. Utilizando el software de PC, alguien puede arrancar una sesión del servidor y acceder a los datos, de nuevo sin conocer un ID de usuario y una contraseña. El riesgo con la emulación 5250 es mayor ya que se necesitan menos conocimientos para arrancar una sesión y empezar a acceder a los datos.

También necesita formar a sus usuarios acerca del efecto de desconectar su sesión de iSeries Access. Muchos usuarios dan por supuesto (lógica pero incorrectamente) que la opción de desconexión detiene completamente la conexión al servidor. De hecho, cuando un usuario selecciona la opción de desconectar, el servidor permite que la sesión (licencia) del usuario esté disponible para otro usuario. No obstante, la conexión del cliente al servidor continúa abierta. Otro usuario podría entrar a

través del PC no protegido y acceder a los recursos del servidor sin haber entrado nunca un ID de usuario y una contraseña.

Puede sugerir dos opciones para los usuarios que necesitan desconectar sus sesiones:

- Asegúrese de que sus PC dispongan de una función de bloqueo que requiera una contraseña. De este modo, un PC desatendido no estará disponible para quien no conozca la contraseña.
- Para desconectar completamente una sesión, finalice la sesión de Windows o reinicie (rearranque) el PC. De este modo concluirá la sesión del iSeries.

También necesita educar a sus usuarios acerca de un riesgo de seguridad potencial cuando utilizan iSeries Access para Windows. Cuando un usuario especifica un UNC (convenio de denominación universal) para identificar un recurso del iSeries, el cliente Win95 o NT crea una conexión de red para enlazar al servidor. Puesto que el usuario especifica un UNC, el usuario no lo ve como una Unidad de red correlacionada. Con frecuencia, el usuario desconoce la existencia de la conexión de red. Sin embargo, esta conexión de red representa un riesgo de seguridad en un PC desatendido, puesto que el servidor aparece en el árbol de directorios del PC. Si la sesión del usuario tiene un perfil de usuario poderoso, los recursos del servidor podrían estar expuestos a riesgos en un PC desatendido. Como en el ejemplo anterior, la solución es asegurar que los usuarios comprendan el riesgo y utilicen la función de bloqueo del PC.

Protección del servidor ante mandatos remotos y procedimientos

Un usuario de PC experto que disponga de software como iSeries Access puede ejecutar mandatos en el servidor sin pasar a través de la pantalla Inicio de sesión. A continuación se detallan varios métodos disponibles para que los usuarios de PC ejecuten los mandatos de servidor. El software de cliente/servidor determina los métodos de que disponen los usuarios de PC.

- Un usuario puede abrir un archivo DDM y utilizar la función de mandato remoto para ejecutar un mandato.
- Parte del software, como los clientes optimizados de iSeries Access, proporciona la función de mandato remoto a través de las API de Llamada de programa distribuido (DPC) sin utilizar DDM.
- Parte del software, tal como ODBC y SQL remoto, proporciona una función de mandato remoto sin DDM o DPC.

Para el software de cliente/servidor que utiliza DDM para el soporte de mandato remoto, puede utilizar el atributo de red DDMACC para evitar totalmente los mandatos remotos. Para el software de cliente/servidor que utiliza otro soporte del servidor, puede registrar los programas de salida para el servidor. Si quiere permitir mandatos remotos, debe asegurarse de que el esquema de autorización sobre objetos protege los datos de forma adecuada. La posibilidad de mandatos remotos es equivalente a proporcionar a un usuario una línea de mandatos. Además, cuando iSeries recibe un mandato remoto a través de DDM, el sistema no aplica el valor Posibilidad limitada (LMTCPB) de los perfiles de usuario.

Protección de estaciones de trabajo ante mandatos remotos y procedimientos

IBM iSeries Access para Windows proporciona la posibilidad de recibir mandatos remotos en el PC. Puede utilizar el mandato Ejecutar mandato remoto (RUNRMTCMD) en el servidor para ejecutar un procedimiento en un PC conectado. La posibilidad de RUNRMTCMD es una herramienta valiosa para los administradores del sistema y el personal auxiliar. Sin embargo, también proporciona la oportunidad de dañar datos de PC, deliberada o accidentalmente.

Los PC no tienen las mismas funciones de autorización sobre objetos que los servidores iSeries. La mejor protección frente a los problemas con el mandato RUNRMTCMD es restringir cuidadosamente los usuarios del sistema que tengan acceso al mandato. IBM iSeries Access para Windows proporciona la posibilidad de registrar a los usuarios que pueden ejecutar mandatos remotos en un PC específico. Cuando la conexión se realiza a través de TCP/IP, puede utilizar el panel de control de propiedades en el cliente para controlar el acceso de mandatos remotos. Puede autorizar a los usuarios por ID de usuario o por nombre de sistema remoto. Cuando la conexión se realiza a través de SNA, determinado software de cliente proporciona la posibilidad de poner a punto la seguridad para la conversación. Con otro tipo de software de cliente, sólo es posible elegir si se pone a punto o no la posibilidad de mandato de entrada.

Para cada combinación de software de cliente y tipo de conexión (como TCP/IP o SNA), es necesario revisar el potencial de los mandatos de entrada para los PC conectados. Consulte la documentación del cliente y busque “mandato de entrada” o “RUNRMTCMD”. Esté preparado para aconsejar a los usuarios de PC y los administradores de red acerca de la forma correcta (segura) de configurar clientes para permitir o evitar esta posibilidad.

Servidores de pasarela

El sistema puede formar parte de una red con un servidor intermedio o de pasarela entre el sistema iSeries y los PC.Por ejemplo, su sistema iSeries puede estar conectado a una LAN con un servidor de PC que tenga PC conectados al servidor.Los elementos de seguridad dependen en esta situación de las posibilidades del software que se ejecuta en el servidor de pasarela. La Figura 13 muestra un ejemplo de una configuración de servidor de pasarela:

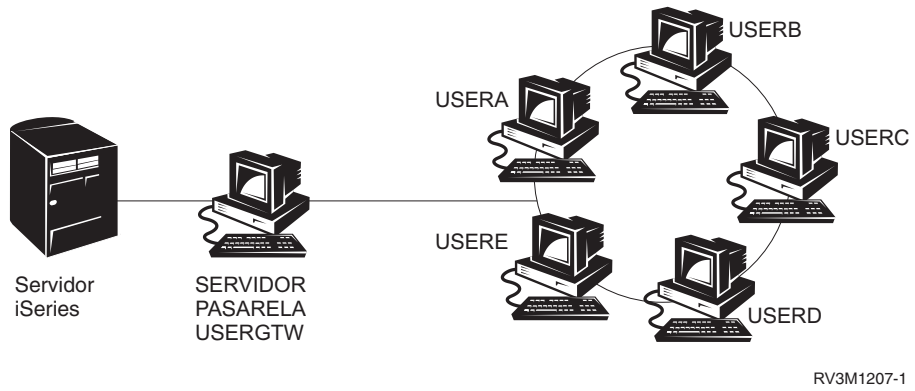

Figura 13. Sistema iSeries con un servidor de pasarela

Con determinado software, el sistema iSeries no conocerá los usuarios (como USERA o USERC) que estén en sentido directo del servidor de pasarela. El servidor iniciará la sesión en el sistema como un sólo usuario (USERGTW). Utilizará el ID de usuario USERGTW para manejar todas las peticiones de los usuarios en sentido directo. Para el servidor una petición de USERA parecerá una petición del usuario USERGTW.

Si es éste el caso, debe confiar en el servidor de pasarela para el cumplimiento de la seguridad. Debe comprender y gestionar las posibilidades de seguridad del servidor de pasarela. Desde la perspectiva de un servidor iSeries, cada usuario tiene la misma autorización que el ID de usuario que utiliza el servidor de pasarela para iniciar la sesión. Un equivalente a esto sería ejecutar un programa que adoptara autorización y proporcionara una línea de mandatos.

Con otro software, el servidor de pasarela pasa las peticiones de los usuarios individuales a servidores iSeries. El servidor iSeries sabe que USERA está solicitando acceso a un objeto determinado. La pasarela es casi transparente para el sistema.

Si el sistema está en una red que tiene servidores de pasarela, debe evaluar qué autorización se debe proporcionar a los ID de usuario utilizados por los servidores de pasarela. También debe comprender lo siguiente:
- Los mecanismos de seguridad que los servidores de pasarela hacen cumplir.
- Cómo aparecen los usuarios en sentido directo ante el sistema iSeries.

Comunicaciones LAN inalámbricas

Algunos clientes pueden utilizar la LAN inalámbrica de iSeries para comunicarse con su sistema sin utilizar cables. La LAN inalámbrica de iSeries utiliza tecnología de comunicaciones por radio frecuencia. Como administrador de seguridad, debe conocer las siguientes características de seguridad de los productos de la LAN inalámbrica de iSeries:

- Estos productos de la LAN inalámbrica utilizan tecnología de difusión de espectro. Esta misma tecnología la utilizó el gobierno en el pasado para asegurar las transmisiones de radio. Para alguien que intente rastrear electrónicamente las transmisiones de datos, éstas parecen ser un ruido, más que una transmisión real.
- La conexión inalámbrica tiene tres parámetros de configuración relevantes para la seguridad:
  - Velocidad de datos (dos velocidades de datos posibles)
  - Frecuencia (cinco frecuencias posibles)
  - Identificador del sistema (8 millones de identificadores posibles)

  Estos elementos de configuración se combinan para proporcionar 80 millones de configuraciones posibles, lo que convierte el hecho de que un pirata informático acierte la configuración correcta en muy poco verosímil.
- Al igual que en el caso de otros métodos de comunicación, la seguridad de las comunicaciones inalámbricas se ve afectada por la seguridad del dispositivo del cliente. La información del ID del sistema y otros parámetros de configuración están en un archivo del dispositivo del cliente y deben protegerse.
- Si un dispositivo inalámbrico se pierde o lo roban, las medidas de seguridad normales del servidor, tales como las contraseñas de inicio de sesión y la seguridad de objetos, proporcionan protección cuando un usuario no autorizado intenta utilizar la unidad perdida o robada para acceder al sistema.

- Si una unidad cliente inalámbrica se pierde o la roban, debe considerar la posibilidad de cambiar la información del ID del sistema para todos los usuarios, puntos de acceso y sistemas. Piense en esto como en cambiar la cerradura de las puertas en caso de que le hayan robado las llaves.
- Probablemente quiera hacer una partición del servidor en grupos de clientes cuyos ID de sistema sean exclusivos. Esto limita el impacto producido por la pérdida o el robo de una unidad. Este método funciona solamente si puede confinar un grupo de usuarios en una parte específica de la instalación.
- Al contrario que la tecnología de LAN por cable, la tecnología de LAN inalámbrica es propietaria. Por lo tanto, no hay rastreadores electrónicos a disposición general para estos productos LAN inalámbricos. Un rastreador es un dispositivo electrónico que lleva a cabo una supervisión no autorizada de una transmisión.

Capítulo 15. Programas de salida de seguridad

Algunas funciones del servidor iSeries proporcionan una salida para que el sistema pueda ejecutar un programa creado por el usuario para realizar comprobaciones y validaciones adicionales. Por ejemplo, puede preparar el sistema para que ejecute un programa de salida cada vez que algún usuario intenta abrir un archivo DDM (gestión de datos distribuidos). Puede utilizar la función de registro para especificar programas de salida que se ejecuten bajo determinadas circunstancias.

Varias publicaciones del iSeries contienen ejemplos de programas de salida que realizan funciones de seguridad.La Tabla 24 proporciona una lista de estos programas de salida, y fuentes de los programas de ejemplo.

Tabla 24. Fuentes de los programas de salida de ejemplo

Tipo de programa de salida	**Finalidad**	**Dónde encontrar ejemplos**
Validación de contraseña	El valor del sistema QPWDVLDPGM puede especificar un nombre de programa o indicar que se utilicen los programas de validación registrados para el punto de salida QIBM_QSY_VLD_PASSWRD para comprobar en las contraseñas nuevas si hay requisitos adicionales que no pueden ser controlados por los valores del sistema QPWDxxx. La utilización de este programa debe supervisarse con suma atención porque recibe contraseñas sin cifrar. Este programa **no debe** almacenar contraseñas en un archivo ni transferirlas a otro programa.	• *An Implementation Guide for iSeries Security and Auditing, GG24–4200* • *iSeries Security Reference*, SC41-5302-07
Acceso a Soporte PC/400 o Client Access[1]	Puede especificar este nombre de programa en el parámetro Acceso de petición de cliente (PCSACC) de los atributos de red para controlar las siguientes funciones: • Función Impresora virtual • Función Transferencia de archivos • Función Carpetas compartidas Tipo 2 • Función Mensajes de Client Access • Colas de datos • Función SQL remoto	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Acceso a Gestión de datos distribuidos (DDM)	Puede especificar este nombre de programa en el parámetro Acceso de petición de DDM (DDMACC) de los atributos de red para controlar las siguientes funciones: • Función Carpetas compartidas Tipo 0 y 1 • Función Someter mandato remoto	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
Inicio de sesión remoto	Puede especificar un programa en el valor del sistema QRMTSIGN para controlar qué usuarios pueden iniciar la sesión automáticamente y desde qué ubicaciones (paso a través.)	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*

Tabla 24. Fuentes de los programas de salida de ejemplo (continuación)

Tipo de programa de salida	Finalidad	Dónde encontrar ejemplos
Conectividad abierta de bases de datos (ODBC) con iSeries Access[1]	Controle las siguientes funciones de ODBC: • Si se permite de alguna manera la ODBC. • Qué funciones se permiten para los archivos de base de datos del iSeries. • Qué sentencias SQL se permiten. • Qué información se puede recuperar acerca de los objetos del servidor de la base de datos. • Qué funciones del catálogo SQL se permiten.	Ninguno disponible.
Programa de manejo de interrupciones QSYSMSG	Puede crear un programa para supervisar la cola de mensajes QSYSMSG y emprender la acción adecuada (como, por ejemplo, notificárselo al administrador del sistema) en función del tipo de mensaje.	*An Implementation Guide for iSeries Security and Auditing, GG24–4200*
TCP/IP	Algunos servidores de TCP/IP (como FTP, TFTP, TELNET y REXEC) proporcionan puntos de salida. Puede añadir programas de salida para manejar el inicio de sesión y para validar peticiones de usuario, como por ejemplo, las peticiones para obtener o colocar un archivo especificado. También puede utilizar estas salidas para proporcionar un protocolo FTP anónimo en el sistema.	"TCP/IP User Exits en la publicación *iSeries System API Reference*"
Cambios del perfil de usuario	Puede crear programas de salida para los siguientes mandatos de perfil de usuario: CHGUSRPRF CRTUSRPRF DLTUSRPRF RSTUSRPRF	• *iSeries Security Reference*, SC41-5302-07 • "TCP/IP User Exits en la publicación *iSeries System API Reference*"

Notas:

1. Encontrará información adicional sobre este tema en el Information Center iSeries. Vea "Requisitos e información relacionada" en la página xii para obtener más detalles.

Capítulo 16. Consideraciones sobre seguridad para los navegadores de Internet

Muchos usuarios de PC de su organización tendrán navegadores en las estaciones de trabajo. Es posible que se conecten a Internet. Es posible también que se conecten al servidor. A continuación se proporcionan algunas consideraciones de seguridad para los PC y para el servidor.

Riesgo: Daños en la estación de trabajo

Una página Web visitada por un usuario puede tener un ″programa″ asociado, como por ejemplo un applet Java, un control Active-X o algún otro tipo de módulo enlazable. Aunque no es el caso habitual, este tipo de ″programas″ pueden dañar la información del PC. Como administrador de seguridad, tenga en cuenta lo siguiente para proteger los PC de la organización:

- Estudie las opciones de seguridad de los distintos navegadores de que dispone. Por ejemplo, en algunos navegadores puede controlar el acceso que los applets Java tienen fuera del navegador (el entorno operativo restringido de Java se llama *sandbox*). Esto puede evitar que los applets dañen los datos del PC.

  Nota: El concepto de sandbox y sus restricciones de seguridad asociadas no existe en Active-X ni en otros módulos enlazables.
- Recomiende a los usuarios los valores a utilizar en el navegador. Probablemente no tenga el tiempo ni los recursos para asegurarse de que los usuarios sigan estas recomendaciones. Por lo tanto debe instruirlos acerca de los riesgos potenciales de la utilización de valores inadecuados.
- Considere la estandarización de los navegadores Web que proporcionan las opciones de seguridad necesarias.
- Haga que los usuarios le informen de cualesquiera comportamientos o síntomas sospechosos que puedan asociarse a sitios Web determinados.

Riesgo: Acceso a directorios de iSeries a través de unidades correlacionadas

Suponga que hay un PC conectado al servidor con una sesión IBM iSeries Access para Windows. La sesión ha configurado unidades correlacionadas para enlazar con el sistema de archivos integrado del iSeries. Por ejemplo, la unidad **G** del PC podría correlacionarse con el sistema de archivos integrado del servidor SYSTEM1 en la red.

Ahora suponga que el mismo usuario de PC tiene un navegador y puede acceder a Internet. El usuario solicita una página Web que ejecuta un ″programa″ perjudicial como puede ser un applet Java applet o un control Active-X. En teoría, el programa podría intentar borrar todo lo contenido en la unidad G del PC.

Existen varias protecciones contra daños en las unidades correlacionadas:

- La protección más importante es la seguridad de recursos en el servidor. El applet Java o el control Active-X tiene para el servidor el mismo aspecto que el usuario que ha establecido la sesión de PC. Necesita gestionar cuidadosamente cuáles son los usuarios de PC que están autorizados a trabajar en el servidor.

- Aconseje a los usuarios de PC que configuren los navegadores para evitar intentos de acceder a las unidades correlacionadas. Esto funciona para los applets Java pero no para los controles Active-X, que no disponen del concepto sandbox.
- Debe instruir a los usuarios acerca del peligro que supone conectarse al servidor y a Internet en la misma sesión. Asegúrese también de que los usuarios de PC (con clientes Windows 95, por ejemplo) comprendan que las unidades permanecen correlacionadas incluso cuando parezca que la sesión de iSeries Access ha finalizado.

Riesgo: Applets firmados de confianza

Probablemente los usuarios hayan seguido el consejo y hayan configurado los navegadores para evitar que los applets graben en unidades de PC. Sin embargo, los usuarios de PC deben tener en cuenta que un *applet firmado* puede alterar temporalmente los valores del navegador.

Un applet firmado lleva asociada una firma digital para establecer su autenticidad. Cuando un usuario accede a una página Web que tiene un applet firmado, el usuario ve un mensaje. El mensaje indica la firma del applet (quién y cuándo lo firmó). Cuando el usuario acepta el applet, el usuario permite al applet pasar por alto los valores de seguridad del navegador. El applet firmado puede grabar en las unidades locales del PC, incluso aunque los valores por omisión del navegador lo impidan. El applet firmado puede también grabar en las unidades correlacionadas del servidor porque para el PC son unidades locales.

Para los applets Java propios procedentes de su servidor, es posible que necesite utilizar applets firmados. Sin embargo, debe indicar a los usuarios que, en general, no acepten applets firmados de origen desconocido.

Capítulo 17. Información relacionada

Manuales

- *APPC Programming*, SC41-5443-00 describe el soporte de comunicaciones avanzadas programa a programa (APPC) para el sistema iSeries. Este manual proporciona ayuda para desarrollar programas de aplicación que utilizan APPC y para definir el entorno para las comunicaciones APPC. Incluye consideraciones sobre el programa de aplicación, requisitos de configuración y mandatos, gestión de problemas para APPC y consideraciones generales sobre gestión de redes. Consulte el CD-ROM iSeries Information Center.
- Libro rojo *AS/400 Internet Security: Protecting Your AS/400 from HARM in the Internet*, SG24-4929 trata los elementos de seguridad y los riesgos asociados a la conexión del iSeries a Internet. Proporciona ejemplos, recomendaciones, consejos y técnicas para las aplicaciones de TCP/IP.
- *Copia de seguridad y recuperación*, SC10-3123-07 (SC41-5304-07) proporciona información sobre la planificación de una estrategia de copia de seguridad y recuperación, salvar información del sistema y recuperar el sistema. Consulte el iSeries Information Center. Encontrará información adicional sobre estos temas en el iSeries Information Center. Vea "Requisitos e información relacionada" en la página xii para obtener más detalles.
- *CL Programming*, SC41-5721-06, proporciona descripciones detalladas para codificar especificaciones de descripción de datos (DDS) para archivos que se pueden describir externamente. Estos archivos son archivos físicos, lógicos, de pantalla, de impresión y de función de comunicaciones intersistemas (ICF). Consulte el iSeries Information Center.
- El tema sobre CL de Information Center (Consulte "Requisitos e información relacionada" en la página xii para obtener más detalles) proporciona una descripción del lenguaje de control (CL) iSeries y sus mandatos OS/400. Los mandatos OS/400 se utilizan para solicitar funciones del programa bajo licencia Operating System/400 (5722-SS1). Todos los mandatos CL que no son de OS/400 (aquellos asociados con los demás programas bajo licencia, incluidos los diversos idiomas y programas de utilidad), están descritos en otros manuales que dan soporte a dichos programas bajo licencia.
- *Implementing iSeriesSecurity, 3rd Edition* by Wayne Madden and Carol Woodbury. Loveland, Colorado: 29th Street Press, a division of Duke Communications International, 1998. Proporciona sugerencias de ayuda y prácticas para planificar, poner a punto y gestionar la seguridad de iSeries.

  Número de pedido ISBN:

  1-882419-78-2
- Para obtener más información sobre el servidor HTTP, consulte el siguiente URL:

  `http://www.ibm.com/eserver/iseries/software/http/docs/doc.htm`
- *iSeries Security Reference*, SC41-5302-07, proporciona información completa acerca de los valores de seguridad del sistema, los perfiles de usuario, la seguridad de recursos y la auditoría de seguridad. Este manual no describe la seguridad de programas bajo licencia, lenguajes y programas de utilidad específicos. Consulte el iSeries Information Center.
- El tema "Operaciones básicas del sistema" de Information Center proporciona información sobre algunos de los conceptos y tareas clave necesarios para las operaciones básicas de iSeries. Vea "Requisitos e información relacionada" en la página xii para obtener más detalles.

- En Information Center se describe cómo utilizar y configurar TCP/IP y las diversas aplicaciones de TCP/IP, por ejemplo FTP, SMTP y TELNET. Vea "Requisitos e información relacionada" en la página xii para obtener más detalles.
- *Soporte de servidor de archivos TCP/IP para OS/400 Installation and User's Guide*, SC41-0125, proporciona información introductoria, instrucciones para la instalación y procedimientos de puesta a punto para la oferta del programa bajo licencia Soporte de servidor de archivos. Explica las funciones disponibles con el producto e incluye ejemplos y sugerencias para utilizarlo con otros sistemas.
- *Trusted Computer Systems Evaluation Criteria* DoD 5200.28.STD, describe los criterios de niveles de confianza para sistemas PC. TCSEC es una publicación del gobierno de los Estados Unidos. Pueden obtenerse copias en:

  Office of Standards and Products
  National Computer Security Center
  Fort Meade, Maryland 20755-6000 EE.UU.
  A la atención de: Chief, Computer Security Standards
- Information Center contiene varios temas relacionados con la Gestión de sistemas y la Gestión de trabajo en el iSeries. Algunos de estos temas incluyen la recogida de datos de rendimiento, la gestión de los valores del sistema y la gestión del almacenamiento. Para obtener detalles sobre cómo acceder a Information Center, consulte "Requisitos e información relacionada" en la página xii. La publicación Gestión de trabajos, SC10-3124-03 (SC41-5306-03), proporciona información sobre cómo crear y modificar un entorno de gestión de trabajos. Consulte el iSeries Information Center.

Además de estos temas de Information Center y los manuales suplementarios, puede utilizar los siguientes recursos para obtener ayuda:

- **IBM SecureWay**
  IBM SecureWay proporciona una marca común para la amplia cartera de ofertas de seguridad de IBM; hardware, software, consultoría y servicios que ayudan a los clientes a proteger su tecnología de la información. Tanto si es para una necesidad individual como para crear una solución total de empresa, las ofertas de IBM SecureWay proporcionan la experiencia necesaria para planificar, diseñar, implementar y operar soluciones seguras para empresas. Para obtener más información acerca de las ofertas de IBM SecureWay, visite la página de presentación de IBM SecureWay:
  `http://www.ibm.com/secureway`
- **Ofertas de servicio**
  Instalar nuevo hardware o software puede producir mejoras en la eficacia y en las operaciones de empresa, pero también plantea la amenaza de interrupciones y anomalías y puede acabar poniendo a prueba sus valiosos recursos internos. IBM Global Services proporciona servicios relacionados con la seguridad de iSeries security. El siguiente sitio Web le permite buscar listados completos de servicios para su iSeries:
  `http://www.as.ibm.com/asus`

Avisos

Esta información se ha escrito para productos y servicios ofrecidos en los EE.UU.

Puede que IBM no ofrezca los productos, servicios o características tratados en este documento en otros países. Consulte al representante de IBM local para obtener información acerca de los productos y servicios disponibles actualmente en su zona. Cualquier referencia a un producto, programa o servicio IBM no implica que únicamente pueda utilizarse dicho producto, programa o servicio IBM. En su lugar, puede utilizarse cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio no IBM.

IBM puede tener patentes o aplicaciones pendientes de patente que cubran información descrita en este documento. La posesión de este documento no le otorga licencia sobre dichas patentes. Puede enviar consultas sobre las licencias, por escrito, a:

| IBM Director of Licensing
| IBM Corporation
| 500 Columbus Avenue
| Thornwood, NY 10594-1785
| EE.UU.

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

| IBM World Trade Asia Corporation
| Licensing
| 2-31 Roppongi 3-chome, Minato-ku
| Tokyo 106, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en que dichas previsiones entren en contradicción con las leyes locales:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITAS NI IMPLÍCITAS, INCLUYENDO, PERO NO LIMITÁNDOSE A LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunos estados no permiten el rechazo de las garantías implícitas o explícitas en determinadas transacciones, por lo que puede que esta declaración no se aplique a su caso.

Esta información puede incluir imprecisiones técnicas o tipográficas. Se efectúan cambios periódicamente a la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en el producto(s) y/o el programa(s) descritos en esta publicación en cualquier momento y sin previo aviso.

Toda referencia en esta información a sitios Web no IBM se proporcionan solamente a efectos ilustrativos, y de ningún modo suponen un endoso a dichos

sitios Web. Los materiales de dichos sitios Web no forman parte de los materiales de este producto IBM y el uso de dichos sitios Web se hará bajo su responsabilidad.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los usuarios licenciados de este programa, que deseen tener información acerca de él a efectos de permitir: (i) el intercambio de información entre programas independientemente creados y otros programas (incluyendo éste), y (ii) el uso mutuo de la información que se haya intercambiado, deberán ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
EE.UU.

Esta información puede estar disponible, sujeta a los correspondientes términos y condiciones, incluyendo en ciertos casos, el pago de una tarifa.

El programa bajo licencia descrito en esta información, y todo el material con licencia disponible para dicho programa, lo ofrece IBM bajo los términos del IBM Customer Agreement, IBM International Program License Agreement, o cualquier acuerdo equivalente entre las dos partes.

Todos los datos de rendimiento aquí contenidos se obtuvieron en un entorno controlado. Por tanto, los resultados obtenidos en otros entornos operativos pueden varias significativamente. Algunas medidas pueden haberse efectuado en sistemas a nivel desarrollo, y no hay garantía de que dichas medidas sean las mismas en los sistemas generalmente disponibles. Además, es posible que alguna medición se haya estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deberían verificar los datos aplicables en sus entornos concretos.

La información concerniente a los productos no IBM se obtuvo de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de acceso público. IBM no ha probado dichos productos y no puede confirmar la exactitud del rendimiento, la compatibilidad ni ninguna otra afirmación relativa a los productos no IBM. Toda cuestión sobre las posibilidades de los productos no IBM deberían ser dirigidas a los suministradores de dichos productos.

Todas las declaraciones relativas a las intenciones o direcciones futuras de IBM están sujetas a cambio o revocación sin previo aviso, y representan solamente metas y objetivos.

Esta información es sólo a efectos de planificación. La información aquí contenida está sujeta a cambio antes de que estén disponibles los productos descritos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen los nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es pura coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que muestran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir dichos programas de ejemplo en cualquier forma sin pago a IBM, para el propósito de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a la interfaz de programación de aplicaciones correspondiente a la plataforma operativa para la que se han escrito los programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. IBM, por consiguiente, no puede garantizar ni implicar la fiabilidad, servicio o funcionamiento de estos programas. Puede copiar, modificar y distribuir dichos programas de ejemplo en cualquier forma sin pago a IBM para el propósito de desarrollar, utilizar, comercializar o distribuir programas de aplicación que se ajusten a las interfaces de programación de aplicaciones de IBM.

Si está examinando esta información mediante una copia software, puede que no aparezcan las fotografías ni las ilustraciones a color.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

Advanced Peer-to-Peer Networking
APPN
AS/400
DB2
DRDA
e (logotipo)
IBMiSeries
Net.Data
Operating System/400
OS/400
PowerPC
SecureWay
System/36
System/38
400

ActionMedia, LANDesk, MMX, Pentium y ProShare son marcas registradas de Intel Corporation en los Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc. en Estados Unidos y/o en otros países.

UNIX es una marca registrada de The Open Group en Estados Unidos y/o en otros países.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas de terceros.

Índice

Caracteres Especiales

A

B

C

CH

D

E

F

G

H

I

J

L

LL

M

N

O

P

Q

R

S

T

U

V

W

Hoja de Comentarios

iSeries
Consejos y herramientas para la seguridad del iSeries
Versión 5

Número de Publicación SC10-3122-07

Por favor, sírvase facilitarnos su opinión sobre esta publicación, tanto a nivel general (organización, contenido, utilidad, facilidad de lectura,...) como a nivel específico (errores u omisiones concretos). Tenga en cuenta que los comentarios que nos envíe deben estar relacionados exclusivamente con la información contenida en este manual y a la forma de presentación de ésta.

Para realizar consultas técnicas o solicitar información acerca de productos y precios, por favor diríjase a su sucursal de IBM, business partner de IBM o concesionario autorizado.

Para preguntas de tipo general, llame a "IBM Responde" (número de teléfono 901 300 000).

Al enviar comentarios a IBM, se garantiza a IBM el derecho no exclusivo de utilizar o distribuir dichos comentarios en la forma que considere apropiada sin incurrir por ello en ninguna obligación con el remitente.

Comentarios:

Gracias por su colaboración.

Para enviar sus comentarios:
- Envíelos por correo a la dirección indicada en el reverso.
- Envíelos por fax al número siguiente: Desde España: (93) 321 61 34
- Envíelos por correo electrónico a: HOJACOM@vnet.ibm.com

Si desea obtener respuesta de IBM, rellene la información siguiente:

Nombre	Dirección
Compañía	
Número de teléfono	Dirección de e-mail

Hoja de Comentarios
SC10-3122-07

IBM España
National Language Solutions Center
Avda. Diagonal, 571
08029 Barcelona

Printed in Denmark by IBM Danmark A/S

SC10-3122-07