

PROGRAMA DE TRABAJO AUDITORIA DE SEGURIDAD LÓGICA iSeries - AS/400

ÍNDICE

1. INTRODUCCIÓN.....	2
2. OBJETIVOS Y ALCANCE.....	3
3. PRUEBAS DE AUDITORIA.....	4
4. ANEXOS	20
4.1. ANEXO I. APLICACIÓN PARA ANALIZAR LA SEGURIDAD LÓGICA DE PERFILES DE USUARIO EN EL SISTEMA AS400....	20
4.2. ANEXO II. MENSAJES RELACIONADOS CON LA SEGURIDAD DEL SISTEMA.....	20
4.3. ANEXO III. TIPOS DE REGISTROS DE LOS EVENTOS DE AUDITORÍA DEL SISTEMA	23

1. INTRODUCCIÓN

El presente programa de trabajo es una guía para determinar el estado de la **seguridad lógica del sistema AS/400**.

El programa de trabajo se ha estructurado en los siguientes módulos:

1. Valores del sistema
2. Perfiles de usuario
3. Protección de objetos y librerías
4. Protección de comandos
5. Protección de trabajos y subsistemas
6. Protección ante accesos desde la red local
7. Copias de seguridad
8. Auditoria de la seguridad

Por cada una de las pruebas a realizar se indica el objetivo de la misma y la información a revisar. En aquellos casos en los que es necesario obtener información del sistema se incluye el comando a ejecutar que nos proporcionará la información necesaria para la revisión.

En los capítulos de “valores del sistema” y “perfiles de usuario” se incluye el parámetro a analizar así como el posible valor recomendado.

Por otro lado, para la realización de las pruebas de los perfiles de usuario, se dispone de una base de datos en Access. Esta herramienta permite, a partir de la información descargada de los perfiles de usuario del sistema AS/400, obtener distintos análisis.

Finalmente se incluyen como anexos los mensajes relacionados con la seguridad del sistema así como los tipos de eventos de auditoria registrados en el diario.

2. OBJETIVOS Y ALCANCE

Objetivos

- Analizar la **seguridad lógica** del sistema AS/400.

El alcance de la revisión se establece en:

- Verificar que los valores establecidos para los parámetros del sistema son los adecuados
- Comprobar que los usuarios y los perfiles asociados a los mismos se encuentran adecuadamente parametrizados.
- Revisar la seguridad de los objetos y librerías de producción para asegurar que solo tienen acceso a las mismas las personas debidamente autorizadas
- Comprobar que se ha restringido el uso de comandos del sistema
- Evaluar la protección existente en los trabajos, subsistemas y en los accesos desde la red local
- Comprobar que se están realizando copias de seguridad tanto de software como de datos, identificando las medidas adoptadas para garantizar su almacenamiento.
- Verificar que la auditoria sobre la seguridad está activa e identificar al responsable de revisar los resultados de la misma.

3. PRUEBAS DE AUDITORIA

Análisis de la Seguridad Lógica en el AS/400

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
SEGURIDAD LÓGICA AS/400		
1. Valores del Sistema		Parámetro (valor recomendado)
Solicitar al administrador la ejecución del comando: WRKSYSVAL SYSVAL (*SEC) OUTPUT (*PRINT) Este comando genera el listado de los valores del sistema asociados a la seguridad. Si se quiere obtener la información en fichero (*FILE)		
Nivel de Seguridad	Comprobar que el valor especificado para el parámetro es ≥ 40 . En los niveles de seguridad 40 o superiores se habilita la seguridad de objetos, recursos y la integridad del sistema operativo. El valor 10 (Physical Security Only) no está soportado en la actualidad. Los niveles posibles de este parámetro son: <ul style="list-style-type: none"> 20 Password security only (Seguridad basada solo en claves) 30 Password and object security (Seguridad basada en claves y objetos) 40 Password, object, and operating system integrity (Integridad en claves, objetos y sistema operativo) 50 Password, object, and enhanced operating system integrity (Integridad avanzada en claves, objeto y sistema operativo) 	QSECURITY (≥ 40)
Características de las contraseñas	Verificar que la longitud mínima de la contraseña (QPWDMINLEN) es igual o superior a 5	QPWDMINLEN (≥ 5)
	Verificar que la longitud máxima de la contraseña (QPWDMAXLEN) es inferior o igual a 10	QPWDMAXLEN (≤ 10)
	Verificar que la caducidad de la contraseña (QPWDEXPITV) es inferior o igual a 60 días. El valor "NOMAX" hace que la contraseña no caduque.	QPWDEXPITV (≤ 60)
	Verificar que se evita el uso de las contraseñas anteriores mas recientes. QPWDRQDDIF (Password re-use cycle) especifica el número de claves previas que OS/400 comprueba para impedir el uso de claves empleadas anteriormente. Por defecto, se permiten claves duplicadas, si bien existe una escala de 8 valores diferentes que permiten recordar al sistema, y por tanto impedir, las últimas 32 claves empleadas.	QPWDRQDDIF (≤ 5)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<p>Identificar los criterios existentes para la confección de contraseñas y si se ha implantado el uso de algún programa de validación de las mismas. (= "n" → Valor recomendado)</p> <ul style="list-style-type: none"> QPWDLMTAJC: Restrict consecutive digits (impide emplear dígitos consecutivos en contraseñas, para evitar claves adivinables, como números de teléfono, DNI, fechas de nacimiento, etc.) El valor 0 desactiva la restricción, con lo que se recomienda que esté activado (= "1") QPWDLMTCHR: Limitador de número de caracteres. Se recomienda que no exista limitación (*NONE) QPWDLMTREP: Limitador de caracteres repetidos en las claves. Se recomienda el valor 2, en el que se prohíbe el empleo de caracteres idénticos consecutivos a la hora de escoger una clave. QPWDPOSDF: Limitador de posición de caracteres. Se recomienda el valor 0 (diferencia posicional no forzada) ya que se considera que limitarlo puede complicar demasiado la elección al usuario: Flower y Andrew no se permitirían por tener la "e" en la misma quinta posición. QPWDRQDDGT: Requerir obligatoriamente dígitos en las claves. Se recomienda el valor (= "1") mediante el cual se obliga a la existencia de dígitos en las claves. QPWDLVDPGM: Indica el programa de validación de contraseñas en uso. Los posibles valores son *NONE (no hay programa de validación en uso), *REGFAC (el nombre del programa de validación se recupera de los datos de registro), nombre_programa (suministrar directamente el nombre del programa de validación, sólo válido si QPWDLVL está a 0 o 1), *LIBL (se emplea una lista de librerías para localizar el programa de validación), *CURLIB (current library, se emplea la librería actual del job para localizar el programa de validación) o nombre_de_librería (librería donde se ubica el programa empleado para la validación de contraseñas) 	<p>QPWDLMTAJC (= "1") QPWDLMTCHR (= *NONE) QPWDLMTREP (= "2") QPWDPOSDF (= "0") QPWDRQDDGT (= "1") QPWDLVDPGM</p>
Seguridad en el acceso al sistema	<p>Verificar que el número de intentos de acceso fallidos (QMAXSIGN) está limitado a un número razonable, nunca superior a 5 intentos fallidos.</p>	<p>QMAXSIGN (<= "5")</p>
	<p>Determinar la acción adoptada (QMAXSGNACN) cuando se sobrepasa el número de intentos de acceso fallidos especificado en el valor anterior. Es recomendable que al menos se bloquee el perfil de usuario ("2") . Las acciones posibles son:</p> <ul style="list-style-type: none"> ("=1") Impedir cualquier otro intento de inicio de sesión para el dispositivo ("=2") Impedir cualquier otro intento de inicio de sesión para el perfil de usuario ("=3") Inhabilitar tanto el perfil de usuario como el dispositivo 	<p>QMAXSGNACN (>= "2")</p>
	<p>Verificar que no se guarda ninguna información de autenticación descifrable. El parámetro QRETSVRSEC determina si se retienen datos relativos a la seguridad del servidor o no:</p> <ul style="list-style-type: none"> ("=0") No se retienen datos de seguridad ("=1") Se retienen datos de seguridad <p>Se recomienda que no se retengan datos</p>	<p>QRETSVRSEC (= "0")</p>
	<p>Verificar que se proporciona al usuario información sobre el último acceso cuando este se conecta al sistema. La información se proporciona si el parámetro QDSPSGNINF está a (= "1"), informándose al usuario sobre la fecha y hora del último acceso, número de accesos erróneos y posibilidad de cambiar la clave. This screen displays the last sign-on date and time, the number of invalid attempts, and permits the user to change their password.</p>	<p>QDSPSGNINF (= "1")</p>
	<p>Verificar que se solicita autenticación para poder acceder de forma remota al sistema. El parámetro QRMTSIGN debe ser (= *FRCSIGNON), de modo que se fuerce el inicio de sesión ante eventos de conexión remota Display Station Passthru, Client Access y TELNET. Se recomienda que este valor no sea *SAMEPRF</p>	<p>QRMTSIGN (= *FRCSIGNON)</p>
	<p>Verificar que la posibilidad de realizar múltiples conexiones simultáneas desde distintos terminales, está restringida a los usuarios debidamente autorizados</p>	<p>QLMTDEVSSN (= "1")</p>
	<p>Identificar si los usuarios con autorizaciones especiales (*ALLOBJ) pueden acceder al sistema desde cualquier Terminal Se recomienda QLMTSECOFR (= "1"), lo que implica que se limita el número de sesiones concurrentes y al control a nivel de perfil de usuario. Los casos donde se permita más de una conexión concurrente (Administradores, otros usuarios privilegiados) deben justificarse.</p>	<p>QLMTSECOFR (= "1")</p>

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
Seguridad de objetos	<p>Verificar que en la autorización de uso público (establecida por defecto para un nuevo objeto creado) no se permite la realización de cambios en dicho objeto. Admite dos valores:</p> <ul style="list-style-type: none"> <i>*USE: Permite acceso a los atributos de objeto y al uso del objeto. El usuario no puede cambiar el objeto.</i> <i>*CHANGE: Permite las operaciones en el objeto a excepción de aquellas limitadas al propietario o sometidas a control de autoridad.</i> <p>Se recomienda que QCRTAUT tenga el valor (=*USE)</p>	QCRTAUT (=*USE)
	<p>Verificar que los usuarios no pueden crear programas que adopten las autorizaciones de otros. Los posibles valores son:</p> <ul style="list-style-type: none"> <i>Nombre_de_lista_de_autorizacion, en el que se establece un nombre de lista de autorización para gestionar la adopción de distintas autorizaciones.</i> <i>*NONE: Valor recomendado, todos los usuarios autorizados por el sistema QUSEADPAUT pueden crear o cambiar programas solo en caso de que los usuarios tengan las autoridades necesarias.</i> 	QUSEADPAUT (=*NONE)
	<p>Verificar si los objetos con seguridad específica pueden ser restaurados en el sistema.</p> <p>Se recomienda el valor *NONE, y los valores *ALWPGMADP y *ALWPTF cuando sea estrictamente necesario.</p>	QALWOBJRST (=*ALL)
	<p>Verificar si se permite la existencia de objetos de dominio de usuario para transferir información entre usuarios. A través de estos objetos, varios usuarios pueden transmitirse información sin pasar por los controles de auditoría y de objeto establecidos en el sistema.</p> <p>El valor de sistema QALWUSRDMN permite la existencia de dominios de usuario y determina qué librerías pueden contener objetos de dominio de usuario. Por defecto, y se recomienda así, el valor es *ALL, si bien es factible que los administradores cambien el valor para especificar una librería o lista de librerías.</p>	QALWUSRDMN (=*ALL)
Control de la auditoría	<p>Verificar que está activa la auditoría sobre el sistema. QAUDCTL es el centro de control principal de la auditoría de seguridad. Su valor por omisión es *NONE, lo que significa que la seguridad no se está auditando. Puede tener otros tres valores posibles:</p> <ul style="list-style-type: none"> <i>*OBJAUD especifica que la auditoría se realizará para determinados objetos. Pueden seleccionarse los objetos que auditar utilizando los mandatos CHGOBJAUD (Cambiar auditoría de objeto) o CHGDLOAUD (Cambiar auditoría de objeto de biblioteca de documentos).</i> <i>*AUDLVL especifica que la auditoría se realizará para las actividades especificadas en el valor del sistema QAUDLVL o en el parámetro AUDLVL de determinados perfiles de usuario, con el mandato CHGUSRAUD (Cambiar auditoría de usuario) se puede especificar que se auditen los usuarios.</i> <i>*NOQTEMP especifica que los objetos de la biblioteca QTEMP no se auditarán. Esta especificación reduce la cantidad de información de auditoría anotada en el diario de auditoría. Los objetos de QTEMP son objetos temporales que se suprimen al finalizar un trabajo, de modo que no auditarlos no debería suponer un riesgo para la seguridad. Deberá especificar *NOQTEMP con *OBJAUD o *AUDLVL; no se puede especificar solo, puesto que la auditoría debe estar activa antes de poder prescindir de los objetos de QTEMP.</i> 	QAUDCTL (=*OBJAUD; *AUDLVL; y *NOQTEMP)
	<p>Identificar la acción a realizar si se llena el log de auditoría. QAUDENDACN es un parámetro que responde a Auditing End Action, Los valores posibles son:</p> <ul style="list-style-type: none"> <i>*NOTIFY (Un mensaje CPI2283 se envía a la cola de mensajes QSYSOPR cada hora hasta que se restablecen los eventos de auditoría)</i> <i>*PWRDWN SYS (Si el sistema no puede escribir registros de auditoría, el sistema se apaga automáticamente)</i> <p>Para el grueso de instalaciones, el valor recomendado es *NOTIFY, con la excepción de máquinas cuyas políticas de seguridad requieran que no se haga ningún procesamiento sin auditoría, en cuyo caso se recomienda *PWRDWN SYS.</p>	QAUDENDACN (=*NOTIFY)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<p>Identificar la frecuencia con que se vuelcan a disco las entradas de auditoria.</p> <p>QAUDFRCLVL hace referencia a <i>Audit Force Level</i>, y es un valor de sistema que permite especificar el número de entradas que serán escritas al registro de auditoria antes de que los datos de entrada sean volcados a almacenamiento auxiliar en disco. Admite dos valores posibles:</p> <ul style="list-style-type: none"> • <i>*SYS (El sistema determina cuando las entradas son movidas a medios auxiliares de almacenamiento, según el desempeño y rendimiento de la máquina)</i> • <i>Número-de-registros (un número de 1 a 100 para especificar el número de eventos de auditoria acumulados en memoria antes de ser llevadas a medio de almacenamiento auxiliar)</i> <p>El valor recomendado es *SYS</p>	QAUDFRCLVL (= *SYS)
	<p>Identificar que al menos los eventos de seguridad (= *AUTFAIL; CREATE; *DELETE; *JOBDDTA; *OBJMGT; *PGMFAIL; *SAVRST; y *SECURITY) son archivados en el log del sistema (notados en negrita). El valor del sistema QAUDLVL determina el nivel de auditoria que se quiere que lleve a cabo el sistema. Hay 16 valores posibles y se pueden especificar tantos como se quieran, mientras no se excluyan mutuamente:</p> <ul style="list-style-type: none"> • <i>*NONE indica que no se realizará la auditoria del sistema, excepto si el valor especificado en el parámetro AUDLVL de sus perfiles de usuario es distinto de *NONE para cada usuario.</i> • <i>*AUTFAIL indica que se auditarán los intentos de inicio de sesión incorrectos y los intentos no autorizados de usar objetos confidenciales. Se incluyen los intentos de conexión rechazados, los intentos de conexión a la red no válidos y los intentos de realizar una operación o de acceder a un objeto para el que el usuario no tiene autorización.</i> • <i>*CREATE indica que se auditará la creación de objetos nuevos o de objetos que sustituyan a objetos ya existentes.</i> • <i>*DELETE indica que se auditarán las operaciones de eliminación de objetos.</i> • <i>*JOBDDTA indica que se auditarán las operaciones de iniciar, cambiar, retener, liberar y finalizar un trabajo. Se incluyen los trabajos de sesiones de servidor y de conexión remota.</i> • <i>*NETCMN indica que se auditarán las violaciones detectadas por el soporte de Filtros APPN.</i> • <i>*OBJMGT indica que se auditarán las operaciones de cambio de nombre y de traslado de objetos.</i> • <i>*OFCSRV indica que se auditarán las tareas de OfficeVision para OS/400 (por ejemplo, cambiar el directorio de distribución del sistema o abrir las anotaciones de correo).</i> • <i>*PGMADP indica que se auditará el acceso a objetos a través de los programas que utilicen autorización adoptada (el sistema anotará en el diario de auditoria las operaciones de inicio y de finalización del programa).</i> • <i>*PGMFAIL indica que se auditarán los programas que ejecuten una instrucción de una interfaz de máquina restringida o que accedan a objetos a través de una interfaz no admitida.</i> • <i>*PRTDDTA indica que se auditará la salida impresa de un trabajo si se envía directamente a una impresora, a un sistema remoto, o que se copia en spool o se imprime en una máquina local.</i> • <i>*SAVRST hace referencia a "The Save/Restore IFSSAVRST", lo que auditará las operaciones de salvado y restauración de los objetos.</i> • <i>*SECURITY indica que se auditará un amplio abanico de actividades relacionadas con la seguridad.</i> • <i>*SERVICE indica que se auditarán las operaciones de iniciar, poner en pausa y parar servidores, y la utilización de las herramientas de servicio.</i> • <i>*SPLFDDTA indica que se auditarán las operaciones de crear, cambiar, retener y liberar archivos en spool. También se anotarán entradas en el diario de auditoria cuando alguien examine un archivo en spool del que no sea su propietario.</i> • <i>*SYSMGT indica que se auditarán las operaciones de cambiar las opciones de copia de seguridad, las opciones de borrado automático, y la planificación de encendido y apagado del equipo utilizando Operational Assistant. También se auditarán los cambios en la lista de respuestas del sistema y en los tiempos de recuperación de la vía de acceso.</i> 	QAUDLVL (= *AUTFAIL; *CREATE; *DELETE; *JOBDDTA; *OBJMGT; *PGMFAIL; *SAVRST; *SECURITY)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<p>Identificar la auditoria por defecto que se aplica a la creación de nuevos objetos. El nivel mínimo aconsejable es *CHANGE, siendo los valores posibles:</p> <ul style="list-style-type: none"> • <i>*NONE (No se realizan acciones de auditoria para el objeto)</i> • <i>*USRPRF (La auditoria del objeto está basada en el perfil del usuario que accede al objeto)</i> • <i>*CHANGE (Siempre que un objeto cambia, se escribe un registro de auditoria)</i> • <i>*ALL (Cualquier acción que afecte a un objeto es registrada en un evento de auditoria. Esta opción incluye a *CHANGE)</i> 	QCRTOBJAUD (= *CHANGE)
2. Perfiles de Usuario		
<p>Solicitar al administrador la ejecución del comando: DSPUSRPRF USRPRF (*ALL) TYPE (*BASIC) OUTPUT (*OUTPUTFILE) Este comando genera el listado de usuarios existentes en el sistema con su perfil y lo descarga en un fichero</p>		
Caducidad de contraseñas	Verificar que el número de usuarios con contraseña caducada no es elevado. El parámetro UPPWEX determina si la contraseña del usuario ha expirado o no.	Parámetro UPPWEX (= *YES)
	Revisar si hay usuarios cuya contraseña no caduca y discutir con el administrador la necesidad de que existan usuarios con dicha característica. El parámetro UPPWEI determina el intervalo de expiración de una contraseña.	Parámetro UPPWEI (= "-1")
	Revisar los usuarios que no han cambiado su contraseña desde una fecha determinada y averiguar si está justificado. El parámetro UPPWCD determina la fecha de último cambio de contraseña.	Parámetro UPPWCD
Perfiles por defecto	Verificar que se han deshabilitado los usuarios que se dan de alta por defecto en la instalación del sistema. El parámetro UPPWON indica si existe contraseña para el perfil.	Parámetro UPPWON (= *YES)
Autorizaciones especiales	<p>Para determinar el nivel o niveles de autorización de cada usuario, debemos recurrir al parámetro de perfil UPSPAU (<i>Special Authorities</i>). Las autorizaciones especiales a revisar son las siguientes:</p> <ul style="list-style-type: none"> • <i>Usuarios con autorización *ALLOBJ (Todos los objetos)</i> • <i>Usuarios con autorización *SAVSYS (Save System)</i> • <i>Usuarios con autorización *SECADM (Security Administrator)</i> • <i>Usuarios con autorización *JOBCTL (Job control)</i> • <i>Usuarios con autorización *SERVICE (Service)</i> • <i>Usuarios con autorización *SPLCTL (Control del Spool)</i> • <i>Usuarios con autorización *ALLOBJ y *SECADM</i> • <i>Usuarios con autorización *AUDIT (Auditoria)</i> 	Parámetro UPSPAU
Menú Inicial	<p>El parámetro UPINMN hace referencia a "initial menu" y determina el menú que se presenta al usuario al iniciar sesión. Los valores posibles son:</p> <ul style="list-style-type: none"> • <i>*MAIN (Se muestra el menú considerado como principal)</i> • <i>*SIGNOFF (El sistema desconecta al usuario una vez termine el programa ejecutado. Es la configuración típica para autorizar a usuarios únicamente a ciertos tipos de programa)</i> 	Parámetro UPINMN Relación y explicación de los menús iniciales existentes distintos a *MAIN y *SIGNOFF
	<p>El parámetro UPINML hace referencia a "Initial Menu Library", y por tanto designa las bibliotecas asignadas al usuario en el momento de iniciar sesión. Las opciones usuales son:</p> <ul style="list-style-type: none"> • <i>*LIBL (Todas las librerías de la lista de librerías para el hilo actual son barridas hasta que se produce la primera coincidencia, siendo esa coincidencia la librería desplegada)</i> • <i>*CURLIB (La librería actual del job es empleada para localizar el programa. Si no se especifica librería para el trabajo, se adopta la librería QGPL)</i> <p>Se deben revisar los usuarios que disponen de una biblioteca inicial distinta a la especificada en QGPL (biblioteca raíz del sistema)</p>	Parámetro UPINML
Programa Inicial	<p>El parámetro UPINPG hace referencia a "Initial Program" y por tanto, identifica el programa inicial. Es frecuente que este parámetro esté a *NONE, lo que indica que no existe un programa inicial asociado.</p> <p>En este punto, se debe obtener el nombre de los programas iniciales existentes y determinar su objeto y justificación.</p>	Parámetro UPINPG Relación y explicación de los programas iniciales existentes
	Identificar la biblioteca que contiene programa inicial de cada usuario. Esto se realiza revisando el parámetro UPINPL, que hace referencia a "Initial Program Library", debiéndose obtener justificación para los distintos casos que se declaren.	Parámetro UPINPL
Capacidad de	El parámetro UPLTCP hace referencia a "Limited Capacity", y	Parámetro UPLTCP

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
operación	<p>determina la capacidad de los usuarios a la hora de operar con la sesión existente. Los valores posibles son:</p> <ul style="list-style-type: none"> • <i>*NO: El programa, menú y librería actual pueden ser cambiados cuando el usuario inicia sesión. Se puede cambiar igualmente la función asociada a la tecla de atención mediante el cambio de perfil. Pueden lanzarse comandos desde la línea de comandos.</i> • <i>*PARTIAL: El programa y librería actual no pueden cambiarse. El menú puede cambiarse y es factible lanzar comandos desde la línea de comandos.</i> • <i>*YES: El programa, menú y librería actual no pueden ser cambiados. No se pueden lanzar comandos desde la línea de comandos. El usuario no puede efectuar cambios.</i> <p>El valor recomendado es *YES (capacidad de operación limitada) siendo posible la existencia de *NO y *PARTIAL, las cuales deben ser justificadas. Deben analizarse los usuarios cuya capacidad de operación no está limitada</p>	(=*NO)
Programa asociado a la tecla de atención	<p>Revisar aquellos usuarios que tengan asignados un programa especial para la tecla de atención. Este programa asociado se especifica mediante el parámetro UPATPG, y deben justificarse los casos aparecidos. Los casos habituales son:</p> <ul style="list-style-type: none"> • <i>*SYSVAL (se toma el programa especificado en QATNPGM, Default Attention Key handling program)</i> • <i>*NONE (No se especifica programa asociado)</i> 	Parámetro UPATPG
Límite de sesiones	<p>El parámetro UPDLVS hace referencia a "Limit Device Session". El objetivo es analizar los usuarios que no tengan establecido un límite al número de sesiones, y que por tanto, pueden tener abiertas simultáneamente en el sistema desde distintos terminales diferentes sesiones. Los valores posibles son:</p> <ul style="list-style-type: none"> • <i>Deselected 0 (No): El sistema admite un número ilimitado de sesiones</i> • <i>Selected 1 (Yes): Los usuarios están limitados a una única session.</i> 	Parámetro UPDLVS (=*NO)
Usuarios inactivos y bloqueados	<p>El parámetro UPSTAT hace referencia a "Status" y ofrece información sobre el estado del perfil de cada usuario. Se deben revisar los usuarios deshabilitados existentes en el sistema y contrastar con el administrador la conveniencia de eliminar dichos usuarios.</p> <p>Los perfiles activos tendrán UPSTAT = *ENABLED, y algunos de estos perfiles activo debe tener los roles QSYS y QSECOFR.</p>	Par. UPSTAT (=*DISABLED)
	<p>El parámetro UPUPLK hace referencia a "User profile locked" y nos ofrece una idea del estado de bloqueo o desbloqueo de los perfiles.</p> <p>Se deben revisar los usuarios bloqueados existentes en el sistema (*LOCKED), averiguar el motivo por el que se han bloqueado y las medidas adoptadas al respecto por el responsable de seguridad.</p>	Par. UPUPLK (=*LOCKED)
Usuarios con clase especial	<p>El parámetro UPUSCL hace referencia a "User Class", y sirve para estratificar a los usuarios en clases. Las clases habituales son:</p> <ul style="list-style-type: none"> • <i>*USER (Usuario)</i> • <i>*SYSOPR (System Operator)</i> • <i>*PGMR (Programmer)</i> • <i>*SECADM (Security Administrator)</i> • <i>*SECOFR (Security Officer)</i> <p>Se debe verificar la idoneidad de la asignación de los usuarios a las distintas clases especiales del sistema. Si alguna de las clases con autorizaciones especiales (SECOFR; SECADM, PGMR...) tiene asignados un número excesivo de usuarios debe discutirse con los responsables, ya que habitualmente es un síntoma de una gestión inadecuada de los usuarios.</p>	Parámetro UPUSCL (User Class)
Último acceso	<p>El parámetro UPPSODR hace referencia a "Previous sign-on date", la última fecha de sign-on al sistema. Deben revisarse los usuarios que no han accedido al sistema desde una fecha no reciente, analizar el estado de los mismos y las acciones adoptadas al respecto.</p>	Parámetro UPPSOD (fecha de último sign-on)
	<p>El parámetro UPPWCD hace referencia a "Password change date". Se deben obtener las fechas de último acceso (UPPSOD) y de cambio de contraseña, identificando aquellos perfiles que debiendo estar deshabilitados no lo estén.</p>	Parámetros UPPSOD y UPPWCD (password change date)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
Propietario de los nuevos objetos creados	Obtener el tipo de propietario de los objetos creados por cada usuario. Los usuarios que tienen el valor GRPPRF (los parámetros suplementales de grupo son GRPPRF y SUPGRPPRF, siendo GRPPRF indicativo de que el perfil de grupo del usuario es propietario de cualquier objeto que el usuario cree), asignan la propiedad del objeto al grupo al que pertenece el usuario, con ello, todos los usuarios de ese grupo tienen control total sobre el objeto. En el caso de * USRPRF, el usuario es propietario de cualquier objeto que haya creado.	Parámetro UPOWNR (Owner)
	UPPGAU es el acrónimo de “User profile group authority”. Se deben identificar los usuarios que al crear un objeto asignan a su grupo principal el permiso *ALL sobre dicho objeto.	Parámetro UPPGRAU (= *ALL)
Grupos sin contraseña	El parámetro UPRPI hace referencia al indicador de perfil de grupo “Group profile indicator” y UPPWON indica si el perfil considerado tiene contraseña definida “Password of none”. Se deben obtener los grupos [UPRPI (= *YES)] que no tienen contraseña de acceso [UPPWON (= *NO)], ya que bajo estas condiciones se puede acceder a través de ellos al sistema.	Parámetros UPRPI (= *YES) + UPPWON (= *NO)
Contraseña trivial	El comando de seguridad ANZDFTPWD: (Analyze Default Passwords) es un comando que enumera claves por defecto en el sistema y que están en espera de una acción en el perfil por parte del usuario (el usuario debe cambiarlas a consecuencia de una pérdida o bloqueo). Deben identificarse los perfiles que estén pendientes de acción y determinar las acciones a tomar.	Ejecutar el comando “ANZDFTPWD”
Inicio de sesión	EL parámetro UPDSIN hace referencia a “Display sign-on information”, y muestra la información que recibe el usuario en el momento de iniciar sesión. El valor recomendado es *YES, con lo que debe determinarse si existen perfiles a los que no se les muestra información en el momento de iniciar sesión.	Parámetro UPDSIN (= *NO)
Grupos asociados al usuario	UPGRPF (Group Profile) indica la posibilidad de que un perfil de usuario herede autoridades especiales de su perfil de grupo. Los valores normales son *NONE, si no hereda propiedades de ningún grupo, o bien el nombre de grupo, si se desea que se hereden de dicho grupo. Se debe identificar el grupo principal asociado al usuario y verificar, si existen, sus autorizaciones especiales, analizando si el usuario debe disponer realmente de las mismas, ya que las hereda de los grupos a los que esté vinculado.	Parámetro UPGRPF
	UPSUPG (Supplemental group) indica la posibilidad de que un perfil de usuario herede autoridades especiales de grupos suplementarios. Deben identificarse los grupos suplementarios asociados al usuario y verificar, si existen, sus autorizaciones especiales, analizando si el usuario debe disponer realmente de las mismas ya que las hereda de dichos grupos.	Parámetro UPSUPG
Auditoría de objetos	En esta prueba se pretende identificar a los usuarios que no tienen definido un nivel de auditoría para los objetos que han creado. Para que la auditoría de objetos entre en acción el valor del sistema QCRTOBJAUD debe estar activado. QCRTOBJAUD permite establecer un valor en el sistema para controlar el valor de auditoría por defecto cuando se crean objetos en una librería. Los posibles valores de QCRTOBJAUD son: <ul style="list-style-type: none"> *NONE, no se hace auditoría alguna para el objeto. *USRPRF, la auditoría del objeto se basa en el valor existente en el perfil del usuario que accede a dicho objeto. *CHANGE, en cuyo caso se escribe un registro de auditoría siempre que un objeto sufra un cambio. *ALL, para cualquier acción que afecte al contenido de un objeto se escribe un registro de auditoría, incluyendo el caso anterior del cambio. Por otro lado, el parámetro UPOBJA (Object auditing value), puede tener los siguientes valores: <ul style="list-style-type: none"> *NONE: No existe un nivel de auditoría para los objetos creados por el usuario. *CHANGE: Existe un nivel de auditoría creado 	Par. UPOBJA (= *NONE)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<p>relacionado con los cambios en los objetos, siempre y cuando el valor de auditoría de objeto QCRTOBJAUD sea *USRPRF.</p> <ul style="list-style-type: none"> *ALL: Si el valor de auditoría de objeto QCRTOBJAUD es *USRPRF, se ha definido un nivel de auditoría tanto para los cambios, como para la lectura. <p>Se recomienda que no se aplique el valor *NONE en el parámetro de perfil de usuario UPOBJA.</p>	
Auditoría del nivel de auditoría sobre acciones	<p>El parámetro UPAUDL hace referencia a "Action auditing value" y representa un valor para el cual se toman acciones determinadas según el valor de auditoría asignado. La prueba está encaminada a identificar usuarios que no tienen definido un nivel de auditoría para sus acciones, y que por tanto, no tienen acciones asociadas.</p> <p>Los valores especificados en este parámetro UPAUDL indican las acciones que se auditarán además de las especificadas en el valor del sistema QAUDLVL, comunes a los usuarios.</p> <p>UPAUDL puede adoptar los siguientes valores:</p> <ul style="list-style-type: none"> Attention events (*ATNEVT) (Eventos de atención del sistema) Authorization failure (*AUTFAIL) (Intentos de inicio de sesión infructuosos en el sistema) Communication and networking tasks (*NETCMN) (Audita violaciones de seguridad acontecidas en el firewall APPN, conexiones por socket, filtros en búsqueda de directorios y violaciones de filtros endpoint) Job tasks (*JOBDA) (Audita acciones que afectan a tareas, tales como iniciar, cancelar, parar, pausar o liberar jobs) Object creation (*CREATE) (Creación o reemplazo de objetos, posibilita monitorizar cuando se crean o recompilan programas, con la excepción de los objetos creados en la librería QTEMP) Object deletion (*DELETE) (Borrado de objetos, audita los objetos externos al sistema borrados, con la excepción de los objetos de la librería QTEMP) Object management (*OBJMGT) (Gestión de objetos, permite auditar objetos renombrados o sujetos al comando move. Útil si queremos detectar la fuga de información sensible, observando si el objeto es movido a otra librería) Object restore (*SAVRST) (Audita la información de salvado y restauración de un objeto, útil para detectar intentos de restauración de objetos no autorizados) Office tasks (*OFCSR) (Audita el software comercial Office Vision) Optical tasks (*OPTICAL) (Auditoría de medios ópticos de almacenamiento, tales como insertar o quitar cartuchos ópticos, o cualquier operación de lectura y escritura efectuada en un medio óptico) Printing functions (*PRTDA) (Para auditar ficheros en cola de impresión. Útil para detectar la impresión de información confidencial) Program adoption (*PGMADP) (Audita la adopción de autoridad para ganar acceso a un objeto determinado) Security tasks (*SECURITY) (Audita eventos de seguridad, como cambios de perfil de usuario o valor de sistema). Service tasks (*SERVICE) (Audita el uso de herramientas de servicio del sistema, como Dumps y Stara Trace) Spool management (*SPLFDA) (Audita las acciones que recibe un objeto en una cola) System integrity violations (*PGMFAIL) (Audita las violaciones contra la integridad del sistema, tales como fallos en validación de valores, violaciones de dominio o instrucciones bloqueadas) System management (*SYSMT) (Auditoría de actividades de gestión del sistema. Debe usarse para detectar intentos de saltar los controles de seguridad a través de las funciones de gestión del sistema) 	Parámetro UPAUDL (=NONE)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<ul style="list-style-type: none"> • <i>Network base tasks (*NETBAS)</i> (Auditoría de transacciones en red, como cambios a reglas IP, estado de la VPN, filtros APPN, etc) • <i>Network cluster tasks (*NETCLU)</i> (Auditoría de operaciones en clusters o en grupos de recursos de cluster. Se entiende cluster como un grupo de uno o más servidores iSeries, o particiones lógicas de un solo servidor, que trabajan como un servidor único) • <i>Network failure (*NETFAIL)</i> (Auditoría de excepciones en comunicaciones, tales como puertos inexistentes a la hora de establecer una comunicación) • <i>Network socket tasks (*NETSCK)</i> (Auditoría de tareas de socket) • <i>Security configuration (*SECCFG)</i> (Auditoría de la configuración de seguridad, tales como modificación de perfiles) • <i>Security directory services (*SEC DIRSRV)</i> (Audita cambios o actualizaciones en funciones del servicio de directorio) • <i>Security interprocess communications (*SECIPC)</i> (Auditoría de las comunicaciones entre procesos) • <i>Security network authentication services (*SECNAS)</i> (Auditoría de eventos de autenticación en red) • <i>Security run time tasks (*SECRUN)</i> (Auditoría del tiempo de ejecución de funciones de seguridad) • <i>Security socket descriptors (*SECCKD)</i> (Audita los intercambios de socket o descriptores de fichero entre dos o más jobs) • <i>Security verification (*SECVFY)</i> (Audita las funciones de verificación, como el cambio del perfil de usuario en un proceso de passthrough) • <i>Security validation tasks (*SECVLDL)</i> (Auditoría de objetos de listas de validación) • <i>Not available (*NOTAVL)</i> (Este valor se muestra si el usuario no tiene autoridad para consultar el valor de auditoría. No se puede invocar manualmente, sólo se produce cuando un usuario que accede al sistema carece de la autorización especial All object (*ALLOBJ) o bien de la autorización especial Audit (*AUDIT) 	
3. Protección de objetos y librerías		
Seguridad en Librerías	<p>Mediante la ejecución de la sentencia <i>Display Object Description (DSPOBJD)</i> aplicado a la totalidad del sistema (*ALL) siendo el tipo de objeto librerías [OBJTYPE(LIB)], obtendremos y verificaremos la lista completa de librerías del sistema.</p> <p>Verificaremos el uso de las librerías del sistema y comprobar que los datos y programas de producción están separados de los de desarrollo.</p>	DSPOBJD OBJ (*ALL) OBJTYPE (*LIB) OUTPUT (*PRINT)
	<p>Seleccionar algunas librerías críticas de producción QSYS, QGPL, QPDA, QPFR, QSVR, listaremos su contenido mediante el comando <i>DSPLIB (Display Library)</i> y verificaremos que sólo contienen datos y programas de producción.</p>	DSPLIB (nombre-librerías-seleccionadas)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<p>Mediante la consulta <i>Display Object Authority</i> (DSPOBJAUT) obtendremos a una lista de usuarios autorizados para las librerías QSYS, QGPL, QPDA, QPFR, QSVR. Comprobaremos que :</p> <ul style="list-style-type: none"> Solamente tienen acceso *CHANGE los usuarios autorizados, estando prohibido el acceso al personal de desarrollo. El propietario es un usuario de producción o un oficial de seguridad <p>En estas librerías, debe comprobarse si se ha establecido como nivel de acceso para *PUBLIC el valor *EXCLUDE, es decir, no se permite el acceso salvo al personal específicamente autorizado.</p>	DSPOBJAUT OBJ (QSYS, QGPL, QPDA, QPFR, QSVR) OBJTYPE (*LIB) o, si se quieren listar todas las librerías, DSPOBJAUT OBJ (*ALL) OBJTYPE (*LIB)
Autorización de acceso a objetos	<p>El comando <i>The Print Adopting Objects</i> (PRTADPOBJ) permite imprimir un informe de los objetos que adoptan autorizaciones especiales y privadas para el perfil de usuario especificado. En este punto, verificaremos que sólo los programas de sistemas (Q*) pueden adoptar las autorizaciones especiales *SECADM, *SECOFR y *SERVICE, debiendo justificarse cualquier otro programa que adopte dichas autorizaciones.</p>	PRTADPOBJ (*ALL)
	<p>Mediante la ejecución de la sentencia <i>Display Object Description</i> (DSPOBJD) aplicado a la totalidad del sistema (*ALL) siendo el tipo de objeto listas de autorización [OBJTYPE(AUTL)], obtendremos y verificaremos todos los objetos de producción que estén protegidos por listas de autorización.</p> <p>Se puede añadir el parámetro DETAIL(*FULL) a la consulta, para obtener una descripción completa (nombre y un conjunto completo de atributos para cada objeto listado)</p>	DSPOBJD OBJ (QSYS / *ALL) OBJTYPE (*AUTL)
	<p>El comando <i>Display Authorization List</i> (DSPAUTL) muestra la lista de usuarios, así como sus niveles de autoridad, que conforman la lista de autorización que estamos analizando. Verificar que los usuarios asociados a las listas de autorización tienen necesidad de acceder al objeto. Nos basaremos en el paso anterior para determinar las listas que nos interesa auditar.</p>	DSPAUTL (nombre-lista)
Autorización de acceso a programas y ficheros	<p>La consulta <i>Display Object Authority</i> (DSPOBJAUT) conduce a una lista de usuarios autorizados para un objeto, así como sus autoridades para dicho objeto. Podemos aplicarla a un objeto del tipo librería o fichero, especificando el tipo de objeto fichero [OBJTYPE (*FILE)] ya que vamos a verificar los ficheros de producción. Verificaremos que únicamente las personas autorizadas pueden acceder a los ficheros de producción.</p>	DSPOBJAUT OBJ (librería/fichero) OBJTYPE (*FILE)
	<p>La consulta es análoga a la anterior, pero en este caso, verificaremos que únicamente las personas autorizadas pueden acceder a los programas de producción.</p>	DSPOBJAUT OBJ (librería/progr.) OBJTYPE (*PGM)
Autorización pública	<p>El comando <i>Print Publicly Authorized Objects</i> (PRTPUBAUT) se emplea para generar un informe en el que se enumeran los objetos que no tienen autoridad pública en *EXCLUDE (es factible un acceso público sin restricción). Aplicaremos la consulta a los objetos fichero, comandos, librerías y programas (*FILE, *CMD, *LIB, *PGM)</p> <p>Este comando imprime dos informes: una lista del tipo de objeto seleccionado donde aparecerán los objetos que no tienen autoridad pública puesta en *EXCLUDE, y un informe secundario de cambios, donde se enumeran los objetos que ahora ya no tienen autoridad pública en *EXCLUDE, pero que sí la tuvieron en algún momento.</p> <p>Verificaremos que los objetos críticos, los confidenciales y los de producción, tienen la autorización pública a *EXCLUDE, es decir, que sin autorización expresa y por tanto, empleando autorizaciones genéricas llamadas públicas, son excluidas.</p>	PRTPUBAUT OBJTYPE (*FILE, *CMD, *LIB, *PGM)
Auditoria	<p>El comando <i>Check Object Integrity</i> (CHKOBJITG) se emplea para revisar si existen violaciones de integridad en el sistema. Puede comprobar falta de integridad en los objetos de los que un perfil de usuario es propietario, en los objetos que concuerden con una ruta determinada del sistema, o si se prefiere, todos los objetos del sistema. Se entiende por violación de integridad:</p> <ul style="list-style-type: none"> Tampering (manipulaciones para esconder accesos no autorizados) en comandos, programas, objetos módulo o atributos de librería. Firmas digitales no válidas en objetos Atributos de dominio inadecuados para el tipo de objeto <p>Mediante el uso de este comando se obtiene un listado de todos los objetos que hayan sido modificados. Se debe obtener una</p>	CHKOBJITG

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	muestra para un periodo determinado y comprobar que todas las actualizaciones están debidamente autorizadas y no comprometen la seguridad del sistema.	
	Mediante la ejecución de la sentencia <i>Display Object Description</i> (DSPOBJD) podemos verificar que los valores de auditoria (OBJAUD) para los objetos críticos y de producción son los adecuados.	DSPOBJD OBJ (nombre)
Procedimientos	Verificar que los cambios son autorizados por los propietarios de los objetos.	N/A
4. Protección de comandos		
Autorización a comandos de seguridad	<p>La consulta <i>Display Object Authority</i> (DSPOBJAUT) conduce a una lista de usuarios autorizados para un objeto, así como sus autoridades para dicho objeto. En este caso, especificaremos el tipo de objeto comando [OBJTYPE (*CMD)] ya que aplicaremos la consulta a los siguientes comandos críticos del sistema:</p> <ul style="list-style-type: none"> •STRSST - Start System Service Tools (muestra el menu System Service Tools (SST)) •WRKOBJ - Work with Objects (muestra una lista de nombres y atributos para los objetos especificados en las librerías especificadas) •SAVSYS - Save System (salva una copia del código interno y la librería QSYS en un formato compatible con la instalación de iSeries) •CRTUSRPRF - Create User Profile (permite identificar usuarios en el sistema y personalizar el modo en el que aparecen) •DLTUSRPRF - Delete User Profile (Elimina del sistema un perfil de usuario) •CHGDSTPWD - Change IBM Service Tools Password (Cambia la clave para las herramientas de servicio proporcionadas por IBM que tengan privilegio de seguridad QSECOFR y las resetea a los valores por defecto) •RSTAUT - Restore Authority (Restaura las autoridades provadas de un perfil) •CHGSYSLIBL - Change System Library List (Cambia la porción de sistema de la lista de librerías para el job en el que se inserta el comando) •RSTUSRPRF - Restore User Profiles (Restaura la información del perfil salvada mediante SAVSYS) •PWRDWN SYS - Power Down System (Inicia la secuencia de apagado de la máquina) •CHGSYSVAL - Change System Value (Cambia el valor de sistema del parámetro seleccionado) <p>En todos los casos, debemos comprobar que los comandos no pueden ser invocados sin autorizaciones expresas, es decir, que su ejecución pública está en *EXCLUDE (exclusión de ejecución)</p>	DSPOBJAUT OBJ (QSYS / nombre-comando) OBJTYPE (*CMD)
	El comando CHGDSTPWD - Change IBM Service Tools Password (Cambia la clave para las herramientas de servicio proporcionadas por IBM que tengan privilegio de seguridad QSECOFR y las resetea a los valores por defecto) sólo debe estar disponible para el perfil de oficial de seguridad. Por tanto, comprobaremos la autoridad del comando y comprobaremos que CHGDSTPWD sólo está disponible para dicho perfil, empleando para ello la consulta <i>Display Object Authority</i> (DSPOBJAUT)	DSPOBJAUT OBJ (QSYS / CHGDSTPWD) OBJTYPE (*CMD)
Autorización de acceso a comandos críticos	<p>Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para obtener una lista de usuarios autorizados para los siguientes comandos críticos:</p> <ul style="list-style-type: none"> •CHGSYSVAL - Change System Value (Cambia el valor de sistema del parámetro seleccionado) •PWRDWN SYS - Power Down System (Inicia la secuencia de apagado de la máquina) •SBMJOB - Submit Job (permite que un job que está siendo ejecutado pueda enviar otro job a una cola, para ser procesado posteriormente en modo batch) 	DSPOBJAUT OBJ (nombre-com.)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
	<ul style="list-style-type: none"> • WRKUSRJOB - Work With User Jobs (Permite trabajar con una lista de jobs de usuario seleccionada) • WRKSPLF - Work with Spooled Files (Permite trabajar con la cola de ficheros seleccionada) • WRKJOBQ - Work with Job Queues (Permite trabajar bien con el estado general de todas las colas de jobs, o bien con el estado detallado de un job determinado) • WRKOUTQ - Work with Output Queues (Permite mostrar y trabajar con el estado general de todas las colas de salida, o bien sólo las que satisfagan unos patrones para los que el usuario está autorizado) • SBMRMTCMD - Submit Remote Command (Envía mediante línea de comando un comando a través del Distributed Data Management (DDM) para ser ejecutado en un sistema destino seleccionado). <p>Es esencial que el acceso a los comandos críticos del sistema está restringido y que el valor para *PUBLIC está en *EXCLUDE</p>	
Autorización de acceso a utilidades restringidas	<p>Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para obtener una lista de usuarios autorizados para las siguientes utilidades restringidas del sistema:</p> <ul style="list-style-type: none"> • STRDFU (Menú principal del Data File Utility) • STRSEU (Start Source Entry Utility, permite editar miembros de ficheros físicos fuente) • STRSDA (Invoca el Screen Design Aid - SDA) • STRPDM (Start PDM, invoca el Programming Development Manager - PDM) <p>Es esencial que el acceso a las utilidades restringidas del sistema está restringido y que el valor para *PUBLIC está en *EXCLUDE, lo que implica que con autorizaciones públicas se produce una exclusión, forzando la aplicación de las deseadas autorizaciones individuales para cada perfil.</p>	DSPOBJAUT OBJ (QSYS / nombre-utilidad) OBJTYPE (*CMD)
Autorización de acceso a utilidades de consulta a bases de datos	<p>Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para obtener una lista de usuarios autorizados para STRQRY (Start Query), empleado para invocar el menú de consulta a base de datos Query/400.</p> <p>Comprobaremos que el acceso a la utilidad Query/400 de consulta a las bases de datos del sistema está restringido y que el valor para *PUBLIC está en *EXCLUDE</p>	DSPOBJAUT OBJ (QSYS / STRQRY) OBJTYPE (*CMD)
Autorización de acceso a ejecutar comandos remotos	<p>El comando SBMRMTCMD - <i>Submit Remote Command</i> envía mediante línea de comando un comando a través del sistema de datos distribuidos <i>Distributed Data Management</i> (DDM) para ser ejecutado en un sistema destino seleccionado.</p> <p>Debemos comprobar que sólo los usuarios autorizados pueden ejecutar comandos remotos (SBMRMTCMD), ya que, por ejemplo, un usuario que acceda a través de soporte PC, podría ejecutar comandos en el sistema aunque no lo puedan hacer directamente en el AS/400. Además, se deberá comprobar que la autorización pública está a *EXCLUDE.</p>	DSPOBJAUT OBJ (SBMRMTCMD) OBJTYPE (*CMD)
Autorización de acceso a comandos de salvado	<p>Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para obtener una lista de usuarios autorizados para los siguientes comandos de salvado del sistema:</p> <ul style="list-style-type: none"> • SAVSTG - Save Storage (Salva el contenido del código interno y los contenidos de los medios auxiliares de almacenamiento a cinta de copia) • SAVSYS - Save System (salva una copia del código interno y la librería QSYS en un formato compatible con la instalación de iSeries) • SAVCFG - Save Configuration (Salva la configuración del sistema y los objetos del gestor de recursos System resource management SRM) • SAVSECDTA - Save Security Data (Salva los mismos datos que SAVSYS, pero incluyendo perfiles de usuario, listas de autorización y mantenedores de autoridad) • SAVLIB - Save Library (Salvar librerías) • SAVCHGOBJ - Save Changed Object (Salva copia de todos los objetos o grupos de objetos cambiados y localizados en la misma librería) <p>Verificar que el acceso a los comandos de salvado del sistema está restringido y que el valor para *PUBLIC está en *EXCLUDE, lo que garantiza que salvo la existencia de autorizaciones específicas, el perfil público está excluido para la ejecución de los comandos de salvado.</p>	DSPOBJAUT OBJ (nombre-comando) OBJTYPE (*CMD)
5. Protección de trabajos (jobs) y subsistemas		

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
Protección de trabajos críticos	Obtener los trabajos críticos activos en el sistema. Para ello aplicamos la consulta <i>Display Object Description</i> (DSPOBJD) aplicada a todos los objetos del sistema (*ALL /*ALL), siendo el tipo de objeto que deseamos los trabajos o jobs (*JOBDD)	DSPOBJD OBJ (*ALL /*ALL) OBJTYPE (*JOBDD)
	Una vez obtenida la lista de jobs críticos, comprobaremos que ningún usuario no autorizado pueda ejecutar algún job bajo un perfil de alta seguridad. Es necesario también comprobar que la configuración asociada a un job no puede ser cambiada si se carece de las pertinentes autorizaciones. Para ello empleamos la consulta de autoridades sobre objetos <i>Display Object Authority</i> (DSPOBJAUT), con la que examinaremos todos los jobs críticos [DSPOBJAUT OBJ (librería / job) OBJTYPE (*JOBDD)], asegurándonos que todos los que tengan definido un perfil en el campo USER tengan la autorización *PUBLIC con el valor *EXCLUDE. Si en el campo USER aparece algún perfil de alta seguridad (QSECOFR, QSYSOPR o QSRV) o algún usuario especial de producción y/o explotación, debe justificarse, comprobando en todo momento que las autorizaciones de los job de producción son las adecuadas para la realización de las funciones que los usuarios desempeñan.	DSPOBJAUT OBJ (librería / job) OBJTYPE (*JOBDD)
Colas de salida	Identificar las colas críticas que contienen ficheros que no se deben modificar o visualizar. Para ello empleamos la consulta <i>Display Object Description</i> (DSPOBJD) aplicada a todos los objetos del sistema (*ALL /*ALL), siendo el tipo de objeto a analizar las colas de salida (Out Queues, *OUTQ)	DSPOBJD (*ALL /*ALL) OBJTYPE (*OUTQ)
	Mediante el comando WRKOUTQD (Work with Output Queue Description) permite trabajar con la descripción informativa de la cola de salida especificada. Así, para cada cola identificada en el punto anterior, ejecutaremos una consulta WRKOUTQD (librería / cola salida) e inspeccionaremos el resultado informativo ofrecido.	WRKOUTQD (librería / cola salida)
	Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para obtener una lista de usuarios autorizados para realizar cambios en las colas de salida. Estos usuarios serán los que tengan autoridad *USE en la librería que contenga la cola, y simultáneamente, alguna de las siguientes autorizaciones: <ul style="list-style-type: none"> Autorización SPLCTL (Spool Control Authority) Autorización JOBCTL (Job Control) y OPRCTL (operator-controlled) en (=YES) Autorización de objeto CHANGE o ALL sobre la cola, autoridad data authority [AUTCHK(=DTAAUT)] y DSPDTA (Display Any Data) en (=YES) 	DSPOBJAUT (librería/ cola salida) OBJTYPE (*OUTQ)
	Comprobaremos que sólo los usuarios autorizados pueden visualizar la información de las colas de salida confidenciales. Estos usuarios serán los que tengan *USE sobre la librería que contenga la cola y una de las siguientes autorizaciones: <ul style="list-style-type: none"> Autorización de objeto CHANGE sobre la cola, autorización de propietario [AUTCHK (=OWNER)] y DSPDTA (Display Any Data) en (=YES) Autorización de objeto USE sobre la cola y DSPDTA (Display Any Data) en (=YES) Autorización de objeto CHANGE sobre la cola y AUTCHK (=DTAAUT) (autoridad data authority) Las autorizaciones recogidas en el punto anterior 	WRKOUTQD (librería / cola salida) DSPOBJAUT (librería/ cola salida) OBJTYPE (*OUTQ)

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
Subsistemas	<p>La primera tarea será identificar los subsistemas existentes, así como sus descripciones. Para ello emplearemos el comando <i>Display Subsystem Description</i> (DSPSBSD) ejecutado sobre todos los subsistemas de la librería QSYS (QSYS/*ALL). Una vez obtenido el listado comprobaremos que:</p> <ul style="list-style-type: none"> • Los sistemas no interactivos (QBATCH, QCMN, QFNC, QDSNX, QSNADS, QSPL) no tienen entradas de estaciones de trabajo. La existencia de dichas entradas los convertiría en interactivos, con lo que los usuarios con suficiente autorización podrían actuar sobre dichos sistemas • Únicamente los sistemas interactivos (QBASE, QCTL, QINTER, QPGMR y QYSSBSD) tienen entradas de estaciones de trabajo. Si no existen dichas entradas los sistemas no son interactivos • Sólo los sistemas interactivos (QBASE, QCTL, QINTER y QYSSBSD) tienen entradas de estaciones de trabajo que especifiquen *CONS (console, sacan información a consola) • Todas las entradas de estaciones de trabajo tienen especificado USER = *RQD, para que los usuarios deban identificarse y autenticarse al conectarse al subsistema (implica que el Default Sign-on no está activo en el sistema) 	DSPSBSD (QSYS / *ALL)
6. Protección de red		
Procesos remotos	<p>Mediante el comando DSPNETA (<i>Display Network Attributes</i>) podemos enumerar los atributos de red del sistema. En esta petición, examinaremos el parámetro JOBACN (acción a tomar por el job para aquellos jobs que se reciben a través de la red). JOBACN puede adoptar los valores *REJECT, *FILE y *SEARCH</p> <ul style="list-style-type: none"> • Si es *REJECT, la petición se rechaza automáticamente. • Si es *FILE, se guarda en un fichero para que el receptor la visualice y decida la acción a llevar a cabo. (visualizar, terminar, recibir o enviar a otra cola de jobs) • Si es *SEARCH, se utiliza la tabla de entrada de jobs de red para determinar la acción a realizar. 	DSPNETA OUTPUT (*PRINT)
	<p>Mediante el comando WRKNETJOBE (<i>Work with Network Job Entry</i>), podemos visualizar las entradas de jobs procedentes de la red. Aprovechando esta información debemos verificar que sólo los usuarios autorizados pueden ejecutar jobs remotos, ya que el comando WRKNETJOBE muestra una entrada por usuario o grupo de usuarios autorizado.</p> <p>Se debe comprobar que dichos perfiles de usuario no proporcionan acceso incontrolado a datos y programas de producción.</p> <p>Verificar que los perfiles no tienen autorizaciones especiales que entrañen peligro para la estabilidad de la seguridad del sistema.</p>	WRKNETJOBE OUTPUT (*PRINT)
Procesos desde la red de PCs	<p>Mediante el comando DSPNETA (<i>Display Network Attributes</i>) podemos enumerar los atributos de red del sistema. En esta petición, examinaremos el parámetro PCSACC (<i>PC Support Access</i>, acción a tomar para peticiones de acceso desde PC vía iSeries Access). PCSACC puede adoptar los valores *REJECT, *OBJAUT, *REGFAC y nombre_programa_acceso:</p> <ul style="list-style-type: none"> • *REJECT implica el rechazo de todas las peticiones de acceso • *OBJAUT implica que las peticiones se aceptan y se controlan mediante las autorizaciones de objeto del sistema • *REGFAC implica que para determinar los programas de salida para los distintos servidores se empleará el registration facility. • nombre_programa_acceso_cualificado indica un nombre de programa suministrado para acceder al AS/400. En este caso habrá que hacer especial hincapié en que el programa y la librería a la que pertenece están adecuadamente protegidos. <p>Dado que la tendencia es que el soporte de PC mediante PCSACC vaya derivando en Client Access, se debe verificar que no se están guardando usuarios ni contraseñas en el fichero STARTPCS.BAT (ni en ningún otro fichero) para realizar accesos remotos automáticos NetWare AS/400 Router y/o similares desde los PCs autorizados. Esta verificación se hará a nivel del software de conexión remota Client Access. La ubicación normal de este fichero es C:\PCS\STARTPCS.BAT</p>	<p>DSPNETA OUTPUT (*PRINT)</p> <p>WRKNETJOBE OUTPUT (*PRINT)</p>

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
Acceso remoto a datos	Mediante el comando DSPNETA (<i>Display Network Attributes</i>) podemos enumerar los atributos de red del sistema. En esta petición, examinaremos el parámetro DDMACC (<i>Distributed Data Management Access</i>), que controla peticiones de acceso remoto desde sistemas distribuidos DDM o DRDA. DDMACC puede adoptar los valores *REJECT, *OBJAUT, y nombre_programa_acceso: <ul style="list-style-type: none"> *REJECT implica el rechazo de todas las peticiones de acceso *OBJAUT implica que las peticiones se aceptan y se controlan mediante las autorizaciones de objeto del sistema nombre_programa_acceso_cualificado indica un nombre del programa cualificado suministrado para acceder al AS/400. En este caso habrá que hacer especial hincapié en que el programa y la librería a la que pertenece están adecuadamente protegidos. 	DSPNETA OUTPUT (*PRINT)
	Se debe comprobar que la librería que contiene las descripciones de los ficheros accedidos remotamente está convenientemente protegida, con acceso restringido a las personas autorizadas y acceso público a *EXCLUDE.	DSPOBJAUT OBJ (nombre) OBJTYPE (*LIB)
Soporte para PC	Verificar que DEFAULT USER (=NONE) y MODE (=QPCSUPP) para no permitir el acceso al sistema mediante el uso del perfil QUSER a través de los subsistemas QCMN o QBASE.	
Dispositivos de comunicación	Afrontaremos dos casuísticas distintas: <p><u>1. Entornos APPC (Advanced Program-to-Program Communication)</u> Ejecutaremos el comando DSPDEVD (<i>Display Device Description</i>) muestra la información descriptiva de un dispositivo que seleccionemos. El parámetro *CMN muestra los contenidos de cada uno de los registros de los distintos recursos de comunicación SRM (<i>Session and Resource Manager</i>) existentes.</p> <p>En una red APPC, y siempre que se emplee DRDA (<i>Distributed Relational Database Architecture</i>), el parámetro SECURELOC se emplea en cada servidor iSeries para indicar si, como posible destino, acepta peticiones de acceso remotas de servidores cuya seguridad ha sido ya verificada, o bien si se requiere usuario y contraseña cifrada. SECURELOC admite los valores:</p> <ul style="list-style-type: none"> *YES *NO *VRYENCPWD, siendo este el mas recomendable, ya que se envía id y contraseña cifrada y el sistema remoto lo verifica para ejecutar el job. <p><u>2. Entornos APPN (Advanced Peer-to-Peer Networking)</u> Ejecutaremos la consulta DSPCFG (Display Configuration List) muestra las entradas de una lista de configuración seleccionada. El parámetro CFGFL indica la lista que queremos consultar, en este caso, la lista de configuración QAPPNRMT.</p>	APPC → DSPDEVD (*CMN) APPN → DSPCFG CFGFL (QAPPNRMT)
7. Copias de seguridad		
Características de las copias de seguridad	Verificar la existencia de procedimientos que determinen los criterios y normas que se van a seguir para la obtención de copias de seguridad. Determinar la periodicidad con que se realizan las copias y el número de copias existentes. Determinar el tiempo durante el que se guardan las copias y el lugar en donde se almacenan. Verificar las condiciones físicas del lugar de almacenamiento.	N/A
Acceso a las copias de seguridad	Identificar que personas tienen acceso a los soportes que contienen las copias de seguridad Comprobar si se ha realizado alguna recuperación de la información contenida en las copias de seguridad y que tipo de registro se efectúa sobre dicha recuperación	N/A
8. Auditoría de la seguridad		
Estado de la auditoría de seguridad	Verificar que la auditoría de seguridad está activada a través de las pruebas ya comentadas en el plan de trabajo: <ul style="list-style-type: none"> Valores de sistema (control de auditoría) Seguridad de librerías y objetos (auditoría de objetos y auditoría de acciones) 	N/A

PRUEBA	ANÁLISIS	DOC. A SOLICITAR
Perfil de usuario por defecto (QDFTOWN)	Verificar que existen procedimientos que revisan y reasignan los objetos propiedad del perfil de usuario por defecto. De forma que los objetos que puedan ser creados bajo dicho perfil tengan un propietario identificado.	N/A
	Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para verificar que los objetos propiedad del perfil propietario por defecto QDFTOWN (<i>Default Owner Profile</i>) tengan su autorización *PUBLIC con el valor *EXCLUDE, de forma que dichos objetos no puedan ser accedidos por cualquier usuario que no cuente con las debidas autorizaciones.	DSPOBJAUT OBJ (*ALL/*ALL) OBJTYPE (*ALL) OWNER (QDFTOWN)
	Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) para verificar que el parámetro *PUBLIC del perfil por defecto sea *EXCLUDE y que únicamente puedan acceder a él las personas que lo necesiten para la gestión y administración del sistema (QSECOFR, QSECADM...)	DSPOBJAUT (QDFTOWN) OBJ (*USRPRF)
Revisión de informes del sistema	Determinar la distribución y revisión de informes de la actividad del sistema referentes a su seguridad lógica. Se debe también determinar cuándo y quién revisa el diario de auditoría.	N/A
Protección del diario de auditoría	Emplearemos la consulta <i>Display Object Authority</i> (DSPOBJAUT) sobre el objeto de sistema QSYS/QAUDJRN, para obtener una lista de usuarios y autorizaciones sobre el diario de auditoría, cuyo tipo de objeto es <i>Journal</i> (*JRN) Una vez obtenido el listado, verificaremos que el diario de auditoría está correctamente protegido contra accesos no autorizados, revisando que el parámetro *PUBLIC sea *EXCLUDE y únicamente tengan acceso los que lo necesiten para realizar su actividad laboral, generándose exclusiones para los perfiles complementarios.	DSPOBJAUT OBJ (QSYS/QAUDJRN) OBJTYPE (*JRN)
Eventos de seguridad del sistema	Mediante la consulta DSPDSTLOG (<i>Display Distribution Log</i>) proporciona un interfaz al log de los servicios de distribución SNADS (<i>Systems Network Architecture Distribution Services</i>). El log SNADS (el diario QSNADS) contiene información sobre operaciones SNADS que han sido ejecutadas en el sistema. Entre estas operaciones están enviar, recibir, distribuciones de ruta y cambios de configuración. En este punto de control, obtendremos una muestra del log QHST (registro de mensajes en un fichero físico denominado log-version, en el que se almacenan trazas de la actividad del sistema, subsistema, información de jobs, estado de los dispositivos y mensajes de operadores del sistema). El objetivo es determinar la presencia de violaciones de seguridad, y que los eventos registrados son representativos. Para ello lanzaremos la consulta DSPDSTLOG LOG (QHST) PERIOD ((fecha inicio) (fecha fin)) MSGID (id mensaje) OUTPUT (*PRINT) Los mensajes relacionados con la seguridad del sistema (id mensaje) más relevantes se encuentran detallados en el anexo 2, siendo pertinente acordar con los usuarios administradores la idoneidad de cada comando.	DSPDSTLOG LOG (QHST) PERIOD ((fecha inicio) (fecha fin)) MSGID (id mensaje) OUTPUT (*PRINT)
Eventos de auditoría del sistema	El comando DSPAUDJRNE (<i>Display Audit Journal Entries</i> (DSPAUDJRNE) permite la generación de informes de auditoría de seguridad del sistema. Aprovecharemos el comando para verificar que los eventos registrados en el diario de auditoría del sistema son correctos, y no corresponden a ningún intento de violación de la seguridad del sistema, Los tipos de entradas que se registran se encuentran recogidos en el anexo 3, se debe verificar al menos las entradas de tipo AF, ND, NE y OR y cualquier otra que se considere relevante para la seguridad del sistema.	DSPAUDJRNE ENTYP (tipo) FROMTIME (fecha inicio) TOTIME (fecha fin) OUTPUT (*PRINT)

4. ANEXOS

4.1. Anexo I. Aplicación para analizar la seguridad lógica de perfiles de usuario en el sistema AS400.

Para la realización de las pruebas de los perfiles de usuario, se puede disponer de una base de datos en Access desde la cual se pueden realizar los filtros adecuados.

4.2. Anexo II. Mensajes relacionados con la seguridad del sistema

CPF1124 → Arranque de job realizado con éxito

CPF1269 → Petición de inicio de Job remota rechazada

CPF1397 → Terminal inhabilitado por el subsistema, debido a que se han superado los intentos máximos de acceso (QMAXSIGN)

CPF1831 → Usuario no autorizado a cambiar el valor del sistema XXX

CPF2117 → XXX Objetos del tipo YYY borrados

CPF2122 → Límite de almacenamiento excedido por el usuario XXX

CPF2130 → XX objetos duplicados // XX objetos no duplicados

CPF2162 → No permitida la duplicación de todos los objetos de la librería XXX

CPF2176 → La librería XXX está dañada

CPF2182 → No autorizado para la librería XXX

CPF2200 → Especifica todos los mensajes de seguridad del sistema; los comprendidos entre CPF2200 y CPF2299

CPF22AD → No se ha encontrado el perfil del grupo especificado

CPF22AF → No autorizado para desplegar objetos asegurados por la lista de autorización XXX

CPF22A5 → Objeto XXX en YYY de tipo ZZZ no está asegurado por la lista de autorización AAA

CPF22A6 v El usuario debe tener autorización *ADD sobre su perfil para poder crear una lista de autorización

CPF22B9 v Usuario no autorizado a modificar las autorizaciones

CPF22C0 → La contraseña indicada no cumple las reglas establecidas por la política de contraseñas

CPF22C2 → La contraseña es menor de XXX caracteres

CPF22C3 → La contraseña es más larga de XXX caracteres

CPF22C4 → La contraseña es igual a una de las 32 contraseñas anteriores

CPF22C6 → La contraseña contiene dos números consecutivos

- CPF22C7 → La contraseña contiene un carácter usado más de una vez
- CPF22C8 → El mismo carácter está en la misma posición que en la contraseña anterior
- CPF22C9 → La contraseña debe contener al menos un dígito
- CPF22D1 → La contraseña no puede ser la misma que el id de usuario
- CPF22D2 → El programa de validación de contraseñas XXX no ha sido encontrado
- CPF22D3 → El programa de validación de contraseñas ha indicado un error
- CPF22D4 → No se permite el uso de un programa de validación de contraseñas
- CPF22D5 → Los parámetros en el programa de validación de contraseñas no son correctos
- CPF22D9 → No existen perfiles de usuario para los nombres indicados
- CPF22E1 → EL parámetro del perfil de usuario USROPT no puede especificar *STSMMSG (los mensajes de estado se muestran por la pantalla cuando son enviados al usuario) y *NOSTSMMSG (los mensajes de estado no se muestran por la pantalla cuando son enviados al usuario)
- CPF2201 → La contraseña del usuario ya existe
- CPF2202 → El usuario no tiene autorización para crear un perfil de usuario
- CPF2203 → El perfil de usuario XXX no es correcto
- CPF2204 → No se ha encontrado el perfil de usuario XXX
- CPF2207 → No está autorizado para utilizar el objeto XXX de tipo YYY de la librería ZZZ
- CPF2209 → No se ha encontrado la librería XXX
- CPF2213 → No se puede ubicar el perfil de usuario XXX
- CPF2216 → No está autorizado a utilizar la librería XXX
- CPF2217 → No está autorizado a utilizar el perfil XXX
- CPF2218 → Intento de acceso al objeto sin autorización
- CPF2219 → Instrucción máquina privilegiada
- CPF2222 → El límite de almacenamiento para el usuario XXX es mayor del especificado
- CPF2223 → No está autorizado para dar autorización sobre el objeto XXX de tipo YYY en la librería ZZZ
- CPF2224 → No está autorizado para revocar autorizaciones sobre el objeto XXX de tipo YYY en la librería ZZZ
- CPF2225 → No es posible ubicar el objeto interno del sistema
- CPF2227 → Se han producido uno o más errores mientras se procesaba el comando
- CPF2228 → No está autorizado a cambiar el perfil de usuario
- CPF2229 → No está autorizado a borrar el perfil de usuario

- CPF2234 → Contraseña no válida
- CPF2237 → No está autorizado para visualizar la lista de usuarios
- CPF2240 → Autorización no adecuada sobre el objeto
- CPF2242 → El objeto XXX de tipo YYY no ha sido encontrado en la librería
- CPF2244 → El objeto XXX de tipo YYY no ha sido encontrado
- CPF2259 → Perfil de grupo XXX no encontrado
- CPF2260 → El perfil de usuario XXX no fue creado / modificado
- CPF2262 → El valor para el parámetro GRPAUT no es correcto
- CPF2264 → El perfil de usuario XXX no puede pertenecer a un grupo
- CPF2266 → El valor *GROUP no está permitido para el perfil de usuario
- CPF2269 → Se requiere la autorización especial *ALLOBJ para conceder autorización *SECADM o *AUDIT a otro usuario
- CPF2272 → No se puede ubicar el perfil de usuario
- CPF2273 → La autorización tal vez no haya sido modificada para el usuario XXX sobre el objeto YYY de tipo ZZZ en la librería AAA
- CPF2278 → La lista de autorización XXX ya existe en el sistema
- CPF2284 → No está autorizado a cambiar la lista de autorización XXX
- CPF2289 → No se puede ubicar la lista de autorización XXX
- CPF2290 → *EXCLUDE no puede estar especificado con otro tipo de autorización
- CPF2294 → El valor del programa inicial no puede ser cambiado
- CPF2295 → EL valor del menú inicial no puede ser cambiado
- CPF2297 → El valor de la librería actual no puede ser cambiado
- CPF2634 → No está autorizado sobre el objeto XXX
- CPF3371 → El SPOOL para el usuario QSPL está dañado o no ha podido ser encontrado
- CPF4104 → El usuario no está autorizado para la operación en el archivo XXX en el YYY miembro, dispositivo o programa de dispositivo
- CPF9802 → No está autorizado para el objeto XXX en YYY
- CPF9805 → El objeto XXX de la librería YYY ha sido destruido
- CPI2236 → Borrado de objetos propios

4.3. Anexo III. Tipos de registros de los eventos de auditoria del sistema

- AF → Fallos de autorización
- CA → Cambios de autorización
- CD → Cadenas de comandos introducidos
- CO → Creación de objetos
- CP → Cambio en los perfiles de usuario
- DO → Borrado de objetos
- JS → Acciones contra jobs del sistema
- ND → Violaciones del filtro de búsqueda en directorios
- NE → Violaciones del filtro del punto final
- OR → Recuperación de objetos
- OW → Cambio de propiedad de objetos
- PG → Cambio del grupo primario de un objeto
- PO → Salidas impresas
- PW → Contraseñas incorrectas
- SF → Acciones sobre los ficheros del spool
- SV → Cambio en los valores del sistema
- VO → Acciones sobre las listas de validación
- YR → Lectura de objetos DLO (objetos de biblioteca de documentos)
- YC → Cambio de objetos DLO
- ZR → Lectura de objeto
- ZC → Cambio de objeto