UNIVERSIDAD POLITÉCNICA DE VALENCIA

Facultad de Informática

IMPLANTACIÓN DE MEJORAS DE SEGURIDAD EN UNA EMPRESA DEL SECTOR FINANCIERO – ASEGURADOR

PROYECTO FIN DE CARRERA

Alumno: **D. Juan Jesús Arroyo Bono**
Director: **D. Antonio Hervás Jorge**
Valencia, Septiembre de 2007

1. Seguridad en los sistemas de Información

1.1. Introducción

La seguridad dentro de una organización no se puede evaluar fácilmente, intervienen muchos aspectos que no siempre son medibles, como por ejemplo los factores humanos.

Las diferentes regulaciones existentes (como el Sabanes-Oxley, ISO-17799, HIPAA, la LOPD, las políticas de retención de la propia organización,…) intentan satisfacer principios de seguridad adaptados a la era actual con el objetivo de poder garantizar que un sistema es “conforme” o “compliance”. Esa denominación de “compliance”, tan de moda en las organizaciones actuales, esconde detrás de sí un trabajo de procedimientación, adecuación de las operaciones, administración, trazabilidad de las transacciones, planes de continuidad de negocio, etc., en fin, un conjunto complejo de entramados de seguridad que muchas veces se pierden en la burocratización de los sistemas, perdiendo incluso el fin para el cual el proceso se puso en marcha: la mejora de la seguridad.

La garantía que nos ofrece una certificación en este tipo de regulaciones no es nada desdeñable, podremos “demostrar” que el sistema es acorde a la regulación que rige el negocio, aunque esto no es nada nuevo. Continuamente vemos sellos de AENOR como que la empresa X esta certificada, pero aún así, es luego cuando internamente se demuestra que no esta tan “certificada”.

En este proyecto tratamos de ser realistas con la seguridad del sistema, no vamos a perdernos en la burocratización del sistema, tampoco vamos a poder manejar toda la complejidad que nos exigen los estándares de regulación internacional, pero si que vamos a poder llevar al sistema a un grado de seguridad aceptable para poder garantizar que nuestra información es “segura”. Este proyecto tiene como punto de partida un análisis previo de la seguridad, con el objetivo claro de poder llevar a cabo las recomendaciones

facilitadas y asegurar que la calidad de las operaciones sobre él están cubiertas.

La calidad de la información en el mundo de la seguridad se rige por lo exacta que es dicha información. Esto no significa demostrar que un datos se almacena en 25 palabras dobles, esto significa que podemos demostrar que el dato es accesible y está disponible, que existe una regulación interna que rige quién puede acceder al dato y cómo puede hacerlo. También que existe una trazabilidad sobre las operaciones del sistema y una garantía de integridad del dato. No vamos a dejar que cualquiera pueda modificarlo, o ni siquiera leerlo, si no está autorizado, que existe coherencia mediante registros y copias de seguridad, que no permitirán mantener nuestro sistema en una situación estable. En definitiva, vamos a garantizar una calidad del sistema de información.

1.2. El punto de partida

Como se ha comentado, el punto de partida es el análisis del sistema actual, donde se ha evaluado el sistema en los siguientes aspectos:

- **Seguridad general**

Se ha evaluado cuál es la configuración general del sistema, conociendo el sistema de seguridad que propone el AS400 se ha obtenido un grado de estado de dicha configuración general, que repercute en todos los objetos y recursos del sistema.

- **Análisis de usuarios**

El análisis de usuarios nos ha permitido observar cual es la jerarquía de usuarios, grupos y su asignación a clases especificas de usuario. También se ha evaluado cual es la gestión que se esta realizando de los usuarios.

- **Seguridad de recursos**

La seguridad de recursos, junto con los usuarios, nos dice quién puede acceder a qué y cómo. Es el aspecto más critico (si hubiera que enunciar alguno) ya que estamos hablando de la realidad en el acceso a la información.

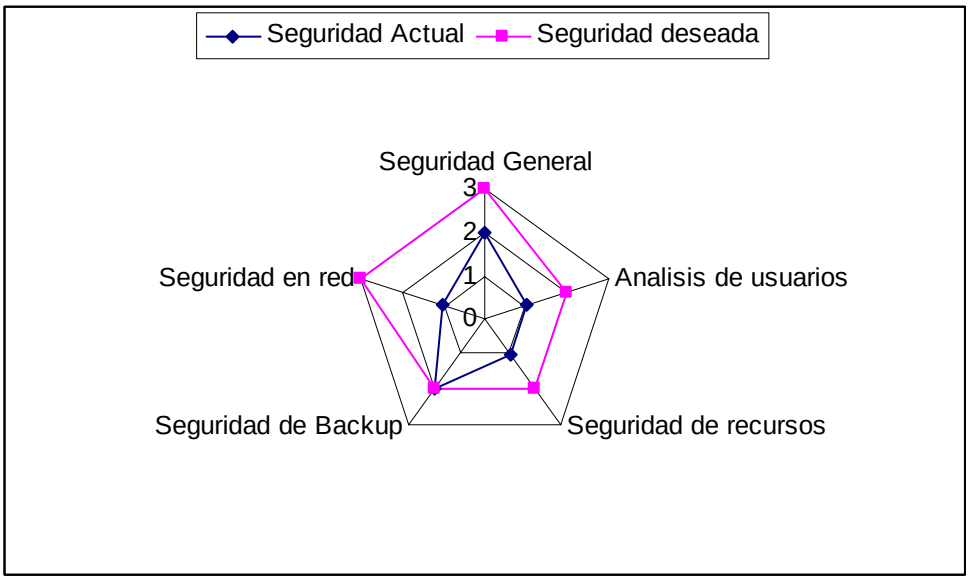
- **Seguridad en copias de seguridad.**

La disponibilidad de los datos en cuanto a la posibilidad de poder recuperar la información y el estado de los sistemas en un momento específico ha sido el objeto de dicha evaluación.

- **Seguridad en red.**

La seguridad en red no solo se basa en que servicios están disponibles para el acceso a la información de forma remota (como ODBC…) sino que también se ha evaluado el sistema de transmisión de datos EDITRAN en cuanto a seguridad se refiere.

Podemos ver el estado actual, comparado con el estado futuro, que queremos obtener representado en el siguiente gráfico, con una escala del 0 al 3 donde 0 es No satisfactorio y 3 es satisfactorio:



1.3. Objetivo

No se va a enumerar cuales son todas las recomendaciones realizadas, pero el objetivo que se persigue es mejorar todas aquellas propiedades del sistema aplicando las recomendaciones realizadas de un modo realista, para que además de ser efectivas no impacten en exceso en el modo de trabajo del sistema.

2. Seguridad general del Sistema

2.1. Introducción

La mayoría de sistemas AS400 han evolucionado desde un escenario en el que se operaba de forma aislada desde terminales “tontas”, lo que permitía una política de seguridad más básica (únicamente se necesitaba gestionar correctamente las claves y los menús del usuario) hacia un sistema “abierto” en el que las conexiones se realizan de forma remota en un entorno cliente-servidor, con unos sistemas abiertos a muchos más usuarios (algunos de ellos demasiado curiosos), también han aumentado las demandas de software más “especializado”, muchas veces comprado a empresas ajenas a IBM, y por último también se ha aumentado la interactividad entre distintos sistemas.

Al mismo tiempo se deberán tener en cuenta que, dada la extensión de la formación informática, el número de posibles atacantes también se ha incrementado (con muy diversas motivaciones: reto personal, ideas políticas, sociales y, por supuesto, el beneficio económico). Aunque frecuentemente las amenazas a la seguridad no procederán de intrusos externos, sino de usuarios autorizados que actúan por error, omisión o mala voluntada.

Otro aspecto a tener en cuenta es que la nueva legislación (LSSI, LOPD,…) nos obliga a controlar todos los aspectos relacionados con nuestros datos (quién los utiliza, cómo e incluso el cuándo de estos accesos).

Estas nuevas características han obligado a modificar y actualizar constantemente las medidas de seguridad no siempre siguiendo un plan de seguridad, sino más bien adecuándola a las nuevas necesidades de cada momento.

2.1.1. ¿Por qué es importante la seguridad?

La información almacenada en el sistema es uno de los valores más importantes del negocio. Hay que tener en mente los tres objetivos más importantes acerca de cómo proteger la información.

Confidencialidad, unas buenas medidas de seguridad pueden evitar que la información llegue a unas manos equivocadas.

Integridad, la información que se tiene en el sistema debe ser correcta. Se debe prevenir el cambio o borrado de datos por usuarios no autorizados.

Disponibilidad, los datos deben estar disponibles para los usuarios, si alguien, intencionadamente o no, daña los datos del sistema, no se podrá acceder a ellos hasta que se hayan recuperado. Un buen sistema de seguridad prevendrá este tipo de daños.

2.1.2. El punto de vista del usuario

También será importante el como afecten estas medidas al usuario, porque el cambio den las medidas de seguridad en algunos casos afectará al cómo utiliza el usuario el sistema y como realiza sus tareas. Por ejemplo, indicar una caducidad de las claves de los usuarios cada cinco días, afectará negativamente en los usuarios e interferirá con su eficacia en su trabajo. Se deberá conseguir un equilibrio entre ambos extremos, pues una política de seguridad demasiado relajada causará serios problemas de seguridad.

2.2. Valores del Sistema

Dentro del ámbito del AS400 los parámetros principales de la configuración se asignan a unas variables especiales del sistema. Estos "valores del sistema" se pueden agrupar en varios tipos:

- Valores de gestión de espacio (*ALC)
- Valores correspondientes a la fecha y la hora (*DATTIM)

- Valores de cambio de valores del sistema (*EDT)
- Valores de registros de mensajes y de logs generados (*MSG)
- Valores de bibliotecas del sistema (*LIBL)
- Valores de seguridad (*SEC)
- Valores de almacenamiento en disco (*STG)
- Valores de control del sistema (*SYSCTL)

De todos estos valores sólo vamos a tratar con los que afectan a la seguridad del sistema, para que se estudie la viabilidad de su cambio y sus posibles implicaciones.

2.2.1. QSECURITY

Este valor del sistema especifica el nivel de seguridad en el que trabaja el sistema.

Al crear un usuario se asignarán los permisos dependiendo del tipo de usuario definido y el nivel en el que se encuentre el sistema.

Esta es la tabla que indica en qué niveles se dará las autorizaciones especiales a un tipo de usuario determinado.

Autorización	**Tipo de usuario**				
	**SECOFR*	**SECADM*	**PGMR*	**SYSOPR*	**USER*
**ALLOBJ*	Todos	10 o 20	10 o 20	10 o 20	10 o 20
**AUDIT*	Todos				
**IOSYSCFG*	Todos				
**JOBCTL*	Todos	10 o 20	10 o 20	Todos	
**SAVSYS*	Todos	10 o 20	10 o 20	Todos	10 o 20
**SECADM*	Todos	Todos			
**SERVICE*	Todos				
**SPLCTL*	Todos				

Otro aspecto al que afectará el nivel del sistema es en la ejecución de ciertas funciones que, dependiendo del nivel en el que se encuentre el sistema, serán permitidas o producirán un error.

Esta es la tabla de diferencias entre los distintos niveles.

Función	**Nivel 20**	**Nivel 30**	**Nivel 40**	**Nivel 50**
Se requiere usuario para el inicio de sesión	Si	Si	Si	Si
Se requiere clave para el inicio de sesión	Si	Si	Si	Si
Activada la seguridad de las claves	Si	Si	Si	Si
Activada la seguridad del menú y del programa inicial	Si	Si	Si	Si
Activada la seguridad de los recursos	No	Si	Si	Si
Acceso a todos los objetos	Si	No	No	No
Perfiles de usuario creados automáticamente	No	No	No	No
Auditoria de seguridad habilitada	Si	Si	Si	Si
No se pueden crear o recompilar programas con instrucciones protegidas	Si	Si	Si	Si
Programas que utilizan interfaces no	No	No	Si	Si

soportadas fallan en tiempo de ejecución				
Soportada protección hardware de almacenamiento	No	No	Si	Si
La librería QTEMP es un objeto temporal	No	No	No	No
*USRSPC, *USRIDX y *USRQ solo pueden ser creados en las bibliotecas especificadas en el valor del sistema QALWUSRDMN	Si	Si	Si	Si
Los punteros usados en los parámetros son validados por el sistema	No	No	Si	Si
Se utilizan reglas en el manejo de mensajes entre el sistema y los procesos del usuario	No	No	No	Si
El espacio de memoria asociado a un programa no puede ser modificado directamente	No	No	Si	Si
Los bloques de control interno están protegidos	No	No	Si	Si

Se recomienda cambiar de nivel 30 a nivel 40.

El cambio de este valor no es un cambio trivial, pues afecta al funcionamiento global del sistema, las aplicaciones pueden dejar de funcionar y los usuarios pueden ver como se deniegan sus accesos a los objetos del sistema por falta de permisos.

Una definición más básica de los niveles sería:

- En el nivel 30, el sistema requiere de un ID de usuario y una clave 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.

- En el nivel 40, el sistema precisa de un ID de usuario y una clave para el inicio de sesión. Además de la seguridad de recursos, el sistema proporciona funciones de protección de integridad, como por ejemplo, la validación de parámetros para interfaces del sistema operativo, estas funciones están dirigidas a proteger el sistema y los objetos del mismo contra una mala utilización por parte de los usuarios experimentados.

2.2.1.1. Comprobaciones previas

Antes de poder realizar el cambio del valor del sistema, se debe asegurar que actualmente no existe ninguna incompatibilidad con el nivel 40 y, en caso de existir, darle solución previamente.

Para identificar los programas que podrían fallar en el cambio de nivel se deberán realizar una serie de pasos:

- Activar la función de auditoria de seguridad del sistema.
- Comprobar que en el valor del sistema QAUDLVL (que controla los eventos que generan anotaciones en el diario de auditoria) se incluye los valores *AUTFAIL y *PGMFAIL (que controlan los fallos de autorización y de integridad del sistema, estos últimos en el nivel 30 son permitidos pero cuando se cambie de nivel se rechazarán).

Hay que prestar atención a las anotaciones del tipo AF:

- B Restricción de acceso a una instrucción del sistema

- C Fallo en la validación de un objeto
- D Interfaz no soportada
- J Descripción de trabajo y/o perfil de usuario no autorizado
- R Intento de acceder a un área protegida del disco
- S Inicio de sesión por defecto

En el nivel 30 los programas sólo producen anotaciones en el diario, el sistema les permite el acceso, pero cuando se produzca el cambio a nivel 40, estos programas dejarán de funcionar.

Ejemplos de acciones que en un nivel 30 serían permitidas (aunque anotadas en el diario de auditoria) y en el nivel 40 el sistema no permitiría su ejecución:

- Un programa intenta acceder a un objeto usando una interfaz no soportada
- Un programa intenta utilizar una instrucción restringida
- Un usuario lanza un trabajo que no tiene permisos *USE sobre el perfil especificado en la descripción de trabajo.
- Un usuario inicia sesión con un usuario sin clave.
- Un programa de usuario intenta escribir en un área del disco que está marcada como solo lectura o de acceso restringido.
- Se produce un intento de realizar algún cambio en las direcciones de memoria asociadas a un trabajo
- Se modifica un comando del sistema (usando el CHGCMD) para que ejecute otro programa en su lugar.

Los tipos de errores que se van a registrar son:

2.2.1.2. Uso de interfaces no soportadas

Los programas pueden pertenecer al dominio de programas de usuario *USER, o de programas del sistema *SYSTEM, en el nivel 40 ningún programa del dominio de *USER se ejecutará en el dominio de *SYSTEM, lo que restringe ciertos accesos a comandos y funciones del sistema.

Al añadir el parámetro *PGMFAIL al valor del sistema QAUDLVL, estos accesos producirán anotaciones tipo AF, subtipo D.

2.2.1.3. Uso de descripciones de trabajo

Si en una descripción de trabajo se indica que debe ejecutarse con un usuario distinto del que lanza el trabajo (parámetro USER), los trabajos ejecutados con dicha descripción se ejecutarán con las propiedades de dicho usuario. Un usuario no autorizado a realizar un acción podría saltarse los controles de seguridad ejecutando un trabajo con una descripción de trabajo que tenga especificado un usuario diferente al suyo.

En el nivel 40, el usuario debería tener permisos de uso (*USE) en la descripción del trabajo y en el perfil de usuario para poder ejecutarlo, en caso contrario el trabajo fallaría. En el nivel 30 es suficiente con tener permisos sobre la descripción del trabajo.

Este tipo de acciones se registran en el diario si el valor del sistema QAUDLVL contiene el parámetro *AUTFAIL. Producirá una anotación de tipo AF subtipo J cada vez que esto suceda.

2.2.1.4. Iniciar sesión sin usuario ni clave

En el nivel de seguridad 30, es posible iniciar sesión sin usuario ni clave bajo ciertas descripciones de subsistemas. En el nivel 40, el sistema deniega cualquier inicio de sesión sin usuario ni clave.

Esta acción deja una notación tipo AF subtipo S en el diario de auditoria.

2.2.1.5. Protección hardware de almacenamiento

Se pueden definir partes del disco como lectura y escritura, solo lectura, o sin acceso. En el nivel 40 el sistema controla como los programas de usuario acceden a estos bloques datos protegidos.

Se añade en el diario de auditoria una anotación tipo AF subtipo R cada vez que se produce un intento de acceso no permitido.

2.2.1.6. Protegiendo el espacio asociado a un programa

En el nivel 40, un programa de usuario no puede directamente cambiar nada del espacio de memoria asociado a un programa en ejecución.

2.2.1.7. Validando parámetros

Las interfaces con el sistema operativo corresponden a programas almacenados en el espacio de usuario que hacen de puente entre los programas del usuario y los del sistema. Cuando los parámetros se pasan entre el espacio de usuario y el espacio del sistema deben ser comprobados para prevenir cualquier valor inesperado que pueda poner en peligro la integridad del sistema.

En el nivel 40, el sistema comprueba específicamente cualquier parámetro que se pasa entre los dos espacios, lo que permite al aumentar significativamente la seguridad del sistema (aunque a costa de un coste en el rendimiento).

También hay que tener en cuenta que si, a pesar de todas las comprobaciones realizadas, tras el cambio el sistema no funciona, se puede volver al nivel 30 de un modo sencillo, sólo será necesario cambiar el valor del sistema a 30 y realizar un IPL.

2.2.2. QLMTDEVSSN

El valor del sistema QLMTDEVSSN especifica si se permite que los usuarios inicien sesión en más de un dispositivo a la vez.

Los valores que acepta son:

- 0 → El sistema permite un ilimitado número de sesiones
- 1 → Los usuarios están limitados a una sesión

La recomendación que se nos hace es cambiar de 0 a 1.

Cambiar este valor del sistema evitaría que ningún usuario pudiese iniciar más de una sesión al mismo tiempo, pero tras estudiar los diferentes grupos de usuarios y sus necesidades se llega a la conclusión que no es una restricción que se pueda generalizar. El modo de trabajo de los usuarios de SEGUROS y PENSIONES requiere de la posibilidad de trabajar en varias sesiones al mismo tiempo, una restricción de este tipo afectaría de manera negativa a su productividad.

Aunque a nivel global no se pueda utilizar esta restricción, es interesante que otros grupos de usuarios de MANTENIMIENTO que disponen de mayores permisos en el sistema observen esta precaución de seguridad. Dado que existe un parámetro en el perfil de usuario que limita el valor máximo de sesiones simultáneas, se procede a añadir la restricción de forma individual a todos los usuarios de los grupos indicados.

2.2.3. QALWOBJRST

El valor del sistema QALWOBJRST determina qué tipo de objetos, que afecten a la seguridad del sistema, pueden ser restaurados. Como por ejemplo aquellos objetos que permiten la adopción de autorizaciones.

Cuando se intenta restaurar un objeto en el sistema, se consultan tres valores del sistema para determinar si se permite el restaurado, o si se realizan modificaciones al objeto restaurado.

El primer filtro es la verificación del objeto (QVFYOBJRST), que se utiliza para controlar el restaurado de algunos objetos que pueden ser firmados digitalmente.

El segundo filtro es el que indica si se debe forzar la conversión en el restaurado (QFRCCVNRST), este valor especifica si se convierten los programas, servicios, paquetes SQL y módulos durante el restaurado.

También puede prevenir el restaurado de algunos objetos. Sólo los objetos que puedan pasar las dos primeras validaciones pasarán esta última validación.

Se puede especificar varios valores de la lista:

- *ALL → Cualquier objeto puede ser restaurado en el sistema por un usuario con las autorizaciones correctas.
- *NONE → Ningún objeto que afecte a la seguridad, como programas del sistema o programas que adoptan autorizaciones, pueden ser restaurados.
- *ALWSYSSTT → Los programas del sistema pueden ser restaurados.
- *ALWPGMADP → Los programas que realizan adopción de autorizaciones pueden ser restaurados en el sistema.

- *ALWPTF → Se permite el restaurado de los objetos durante la aplicación de PTF (actualizaciones) en el sistema.
- *ALWSETUID → Se permite el restaurado de ficheros con el atributo S_ISUID habilitado.
- *ALWSETGID → Se permite el restaurado de ficheros con el atributo S_ISGID habilitado.
- *ALWVLDERR → Se permite el restaurado de ficheros que no han superado los tests de validación de objetos. Si se ha especificado el valor del sistema QFRCCVNRST el objeto será corregido para que supere las validaciones.

*Se recomienda cambiar de *ALWPTF a *NONE*

La instalación del software de terceros necesita que este valor del sistema esté en *ALL, e incluso las actualizaciones del sistema requieren como mínimo que el parámetro esté en *ALWPTF. Como se trata de procedimientos muy puntuales y realizados la mayoría de veces sin que existan usuarios conectados al sistema, se cambia el valor a *NONE y se modifican los procedimientos para que se cambie a *ALL cuando sea necesario (volviéndose a poner en *NONE al finalizar la instalación).

2.2.4. QAUTOCFG

Este valor del sistema permite que el sistema configure, y cree si son necesarios, automáticamente los dispositivos conectados.

Los valores posibles son:

- 0 → No existe configuración automática. Se deben crear manualmente los dispositivos que se añadan al sistema.
- 1 → Configuración automática habilitada. El sistema creará, si es necesario, y configurará los dispositivos que se añadan al sistema. Se enviará un mensaje al operador con el cambio que se realice.

Se recomienda cambiar de 1 a 0.

Es una situación habitual la creación de nuevos dispositivos por parte del sistema, principalmente en dos contextos.

A los usuarios, al iniciar sesión, se les asigna un dispositivo virtual de pantalla, este dispositivo, llamado QPADEVxxxx, se asigna automáticamente y en caso de no existir, se crea uno nuevo. Cada sesión que tenga el usuario con el sistema necesitará de un nuevo dispositivo. No es posible controlar el número de dispositivos necesarios en el sistema, por lo que en este caso la creación automática es necesaria.

El software cliente de los sistemas permite imprimir utilizando las impresoras conectadas localmente al usuario, esto lo realiza creando impresoras virtuales que hacen de nexo entre el sistema remoto y el local. Los usuarios deben poder conectar sus propias impresoras al sistema y, por lo tanto, de nuevo se hace necesaria la creación automática de dispositivos en el sistema.

Tras estudiar las repercusiones del cambio en el valor del sistema, se descarta el cambio recomendado.

2.2.5. QAUTOVRT

Este valor del sistema especifica el número de dispositivos virtuales que se pueden crear automáticamente en el sistema.

Los valores posibles son:

- 0 → No se crea automáticamente ningún dispositivo virtual
- Número → Con un valor entre 1 y 9.999. Si al iniciar sesión, existe un número de dispositivos menor a los indicados y no existe ninguno disponible, el sistema automáticamente creará y configurará uno nuevo.

Se recomienda cambiar de 256 a 0.

Como ya se ha comentado anteriormente (en el apartado QAUTOCFG), el modo de trabajo actual en el sistema requiere de la creación automática de los dispositivos virtuales por lo que no se puede poner a 0 este valor. Se considera adecuado a las necesidades actuales el valor de 256.

2.2.6. QDEVRCYACN

Este valor indica las acciones a tomar cuando ocurre un error de tipo entrada/salida en la estación de trabajo de un usuario interactivo.

Los valores posibles son:

- *DSCMSG → Se desconecta el trabajo. Cuando se inicia sesión de nuevo, se envía un mensaje de error al programa del usuario.
- *MSG → Se notifica el error al programa del usuario. Dicho programa realizará la recuperación del error.
- *DSCENDRQS → Se desconecta el trabajo. Al iniciar de nuevo la sesión, se envía un mensaje de cancelación al programa del usuario.
- *ENDJOB → Finaliza el trabajo. Se genera un informe del trabajo. SE envía un mensaje indicando que el trabajo ha finalizado porque ha existido un error en el dispositivo. Para minimizar el rendimiento del trabajo en su finalización, se disminuye en 10 la prioridad del trabajo.
- *ENDJOBNOLIST → Finaliza el trabajo. No se genera un informe del trabajo. Se envía un mensaje indicando la finalización del trabajo debida a un error en el dispositivo.

Cuando se indica el valor *MSG o *DSCMSG, la acción de recuperación no se realiza hasta la siguiente operación de entrada/salida del trabajo. En un entorno cliente/servidor, permite que, si se conecta desde la misma dirección IP, antes de que el trabajo realice la siguiente operación de entrada/salida, el trabajo puede recuperarse del mensaje de error y seguir funcionando en el segundo dispositivo.

Para evitar esto, se debe gestionar la acción de recuperación con los valores *DSCENDRQS, *ENDJOB o *ENDJOBNOLIST, ya que estas acciones serán ejecutadas inmediatamente a la generación del error.

*Se recomienda cambiar de *ENDJOBNOLIST a *DSCMSG*

Al indicar el valor *DSCMSG se han detectado casos en los que el trabajo no se finaliza nunca, por lo que se considera necesario la finalización del trabajo con *ENDJOB o *ENDJOBNOLIST. Tras consultarlo con los diferentes grupos de usuarios se descarta la necesidad de tener un informe con la finalización del trabajo, por lo que se mantiene el valor de *ENDJOBNOLIST.

2.2.7. QPWDLVL

Este valor indica las restricciones que se aplican a las claves de los usuarios.

Los parámetros que acepta el valor del sistema QPWDLVL son:

- 0 → Las claves de los usuarios tienen una longitud de 1 a 10, y los caracteres que se aceptan son 'A-Z', '0-9', '$', '@', '#' y '_'.
- 1 → Además de las restricciones del valor 0, se eliminan las claves de los clientes iSeries Netserver para los sistemas operativos Microsoft Windows 95/98/ME.
- 2 → Se permiten claves de 1 a 128 caracteres, se aceptan todos los caracteres. La clave es sensible a las mayúsculas y minúsculas. Este valor es el más compatible pues permite que se conecten los clientes del iSeries Netserver.
- 3 → Este valor permite la flexibilidad de las claves del valor 2, añadiendo las restricciones de no conexión con los clientes iSeries Netserver y tampoco con aquellos sistemas AS400 que tengan este valor del sistema a 0 o 1.

Se recomienda cambiara de 0 a 2.

Siguiendo las recomendaciones se cambia al valor 2.

2.2.8. QPWDLMTAJC

Este valor limita la posibilidad de que existan dígitos adyacentes en una clave. Sirve para prevenir que los usuarios utilicen fechas, números de teléfono o una secuencia de números como claves.

Los parámetros que permite son:

- 0 → Se permite que existan números adyacentes en una clave.
- 1 → No se permiten números adyacentes en las claves.

Se recomienda cambiar de 0 a 1.

Se considera una restricción excesiva dado que se limitan en excesivo las posibilidades de las claves y, probablemente, afectaría negativamente a los usuarios.

2.2.9. QPWDLMTREP

Este valor del sistema limita el uso de caracteres repetidos en una clave. Este valor previene claves fáciles de adivinar, como el mismo carácter repetido varias veces.

Valores que puede tener:

- 0 → Se puede usar el mismo carácter más de una vez en una clave.
- 1 → El mismo carácter no puede ser usado más de una vez en una clave.
- 2 → El mismo carácter no puede ser usado consecutivamente un una clave.

Ejemplos de claves:

Clave	QPWDLMTREP = 0	QPWDLMTREP = 1	QPWDLMTREP = 2
Q22222	Permitida	No permitida	No permitida
JOSSE	Permitida	No permitida	No permitida
AUTOBUS	Permitida	No permitida	Permitida
N707SP	Permitida	No permitida	Permitida

Se recomienda cambiar de 0 a 2.

Se considera que este cambio no afecta excesivamente a los usuarios y aumenta la seguridad del sistema, por lo que se cambia a 2 el valor del sistema.

2.2.10. QPWDRQDDIF

Este valor del sistema controla cuando se podrá utilizar de nuevo una clave. Evita que cuando caduca una clave se cambie inmediatamente por la vieja.

Los valores que acepta son:

- 0 → Permite claves iguales.
- 1 → La nueva clave debe ser diferente a las 32 anteriores.
- 2 → La nueva clave debe ser diferente a las 24 anteriores.
- 3 → La nueva clave debe ser diferente a las 18 anteriores.
- 4 → La nueva clave debe ser diferente a las 12 anteriores.
- 5 → La nueva clave debe ser diferente a las 10 anteriores.
- 6 → La nueva clave debe ser diferente a las 8 anteriores.
- 7 → La nueva clave debe ser diferente a las 6 anteriores.
- 8 → La nueva clave debe ser diferente a las 4 anteriores.

Se recomienda cambiar de 8 a 5.

Dado que las claves caducan cada 30 días el nuevo valor del sistema evita que se repitan las 10 anteriores, lo que no permite que se mantengan claves diferentes durante 10 meses (anteriormente se mantenían durante 4 meses). Se sigue la recomendación y se cambia el valor del sistema a 5.

2.2.11. QAUDCTL

Este valor del sistema indica qué tipo de información debe ser auditada.

Los parámetros pueden ser:

- *NONE → No se audita.
- *OBJAUD → Se auditan aquellos objetos en los que se ha indicado manualmente que se deben auditar.
- *AUDLVL → Se auditan aquellas acciones indicadas en los valores del sistema QAUDLVL y QAUDLVL2, o aquellos usuarios en los que el parámetro AUDLVL de su perfil de usuario se ha indicado algún valor distinto de *NONE.
- *NOQTEMP → No se auditan aquellas acciones realizadas sobre la biblioteca QTEMP (biblioteca temporal del usuario).

*Se recomienda añadir *NOQTEMP.*

Dado que, mientras el usuario está conectado, esta biblioteca se puede utilizar como biblioteca de trabajo, también es necesario mantener un registro de las acciones realizadas en ella. En caso contrario se produciría un vacío en aquellas acciones que el usuario realizara en esta biblioteca dejando así, una posible vulnerabilidad en el sistema. Por estos motivos, no se añade *NOQTEMP al valor del sistema.

2.2.12. QRETSVRSEC

Este valor del sistema indica si la información de encriptación asociada a los perfiles de usuario o las entradas de las listas de validación puede ser obtenida remotamente. No se incluye la clave del usuario.

Los valores que acepta son:

- 0 → No se recupera la información.
- 1 → Se puede recuperar la información.

Se recomienda cambiar de 1 a 0.

Para dificultar la labor a un atacante externo, es importante minimizar la cantidad de información que se puede obtener del sistema. Se sigue la recomendación y se pone en 0 el valor.

2.3. Otras recomendaciones

2.3.1. Inhabilitación de perfiles fuera de horario de oficina

Para los usuarios de los grupos de SEGUROS y de PENSIONES ya existe una inhabilitación de los usuarios dada la incompatibilidad de sus tareas con las realizadas en horario “BATCH”. Pero siguiendo la recomendación de inhabilitar los usuarios fuera del horario de oficina, se realizan varias reuniones con el resto de grupos de usuarios.

Al finalizar las reuniones se llega a la conclusión de que no se puede definir de una manera sencilla cuál es el horario “normal” de trabajo ya que existen usuarios que, perteneciendo al mismo grupo, tienen distintos horarios de trabajo. También se está volviendo una práctica “habitual” que los usuarios se conecten fuera de horario para finalizar las tareas que se consideran más urgentes.

Sin embargo existe una serie de usuarios de Mantenimiento, que realizan guardias nocturnas con unos usuarios con más permisos de los habituales. A estos usuarios se les restringirá el acceso en horario de oficina.

2.3.2. Cambiar mensajes CPF1107 y CPF1120

Siguiendo la recomendación se cambian los textos de los mensajes quedando ambos errores con el siguiente mensaje de error: “La información de inicio de sesión no es correcta”.

2.3.3. Autorización adoptada

En el apartado de los usuarios para reducir la cantidad de permisos de los diferentes grupos de usuarios, se realizarán adopciones de autorización para ejecutar aquellas tareas “puntuales” que requieran permisos adicionales. Por este motivo el control de estas autorizaciones se realizará en ese apartado.

2.4. Análisis

En general el estado del sistema era el correcto. El informe de recomendaciones ha presentado algunos valores del sistema (que aunque son de bajo impacto en la seguridad) son recomendables que se corrijan, así como situaciones que ya estaban detectadas y que, dado el modo de trabajo actual, no se pueden cambiar y se asumen como riesgos.

Una recomendación importante que se ha tenido en cuenta es el cambio del nivel de seguridad (QSECURITY) de 30 a 40, que, aunque ha requerido un esfuerzo y una dedicación importantes, la gran mejora en la seguridad del sistema que se ha producido, justifica sobradamente el trabajo invertido.

3. Gestión de usuarios

3.1. Introducción

Una de las deficiencias encontradas en el sistema es la configuración de los usuarios. Al no existir una política de usuarios clara, la creación de usuarios ha evolucionado a lo largo del tiempo con nuevos requisitos, muchas veces dependientes del “buen hacer” de la persona que realiza el alta. Esto, a lo largo del tiempo, ha generado diferencias importantes en los perfiles de usuario.

También hay que tener en cuenta que el aumento de usuarios ha convertido las tareas de mantenimiento de los mismos, que habitualmente eran manuales, en unas tareas largas y tediosas que al final no se realizan con la frecuencia que debieran.

Tras la creación de los procedimientos también será necesaria, dentro del ámbito de los AS400, la creación de una herramienta que facilite la aplicación de estas políticas y su mantenimiento.

También hay que tener en cuenta la recomendación de eliminar el permisos *ALLOBJ de todos los usuarios del sistema. Esto provocará que la existencia de una correcta asignación de permisos se vuelva una tarea crítica y que se deba realizar un estudio pormenorizado de aquellas acciones de los usuarios que requieren de permisos “adicionales”. Este tema será tratado en profundidad en posteriores capítulos.

3.2. Políticas de usuario

Un aspecto importante para lograr un alto nivel de seguridad informática es la educación y la formación.

En términos sencillos, una política de seguridad es un listado en el que se detalla qué se debe hacer y como se debe hacer en materia de seguridad de la información.

Existen procedimientos que, dada su importancia en la seguridad de un sistema, deben estar definidos de una manera clara, de este modo se conseguirá que tanto aquellos que ejecutan el procedimiento como aquellos que se ven afectados tengan claro qué se ha hecho, cómo e incluso el porqué.

3.2.1. Alta de usuarios

Para dar de alta un usuario se deberá utilizar la aplicación de usuarios (el procedimiento se detalla más adelante).

Se deberá tener en cuenta ciertas consideraciones:

- Cualquier alta de usuario debe ser solicitada por la Oficina Técnica, excepto los usuarios de Mantenimiento e Impresión que pueden ser solicitados por los jefes de proyecto, siendo requisito indispensable que la petición esté aprobada por el responsable del departamento de Mantenimiento.

- La clave no se cumplimentará en la petición y nunca deberá ser la misma que el nombre del usuario. Se enviará por correo al usuario.

- Los usuarios se configurarán de modo que sea obligatorio el cambio de clave en su primer inicio de sesión (este punto se implementará en la aplicación de usuarios).

- Todos los perfiles de usuario deben tener como descripción el nombre y apellidos de la persona a la que está asociado el perfil de usuario.

3.2.2. Baja de usuarios

Para dar de baja un usuario también se deberá utilizar la aplicación de usuarios (el procedimiento se detalla más adelante).

Se deberá tener en cuenta:

2. Las bajas de usuario deben ser solicitadas por la Oficina de Proyectos. La oficina pedirá la baja de un usuario mediante una Solicitud de Mantenimiento.

3. Para realizar la baja de un usuario deberán buscarse todos sus perfiles y darlos de baja con la Aplicación de Usuarios. De esta manera quedará registrada en los informes generados por la herramienta de Aplicación de Usuarios.

3.3. Aplicación de usuarios

3.3.1. Introducción

Se requiere una aplicación que gestione y automatice en lo posible la gestión de usuarios en el AS400. Esta aplicación constará de una parte interactiva, con mantenimiento de perfiles de usuarios y grupos, cambios de grupo, bloqueo/desbloqueo de usuarios, creación de informes, etc. Y de una parte “batch” que gestionará automáticamente el bloqueo y desbloqueo de usuarios que empiezan o terminan periodos de vacaciones o de consulta, bloqueo de usuarios que no han iniciado sesión en un determinado número de días o borrado de los usuarios que llevan n días bloqueados.

3.3.2. Funcionamiento

Al crear un usuario se grabará un registro en el maestro de usuarios con los datos básicos para gestionar su perfil desde la aplicación. Entre los datos que se graban en este fichero al crear un perfil están el identificador de usuario y el grupo al que pertenece. La aplicación creará el perfil con una clave “caducada” (será necesario su cambio en el primer inicio de sesión) generada por la propia aplicación, de la que será informado el usuario administrador de la aplicación para que éste la mande al usuario final.

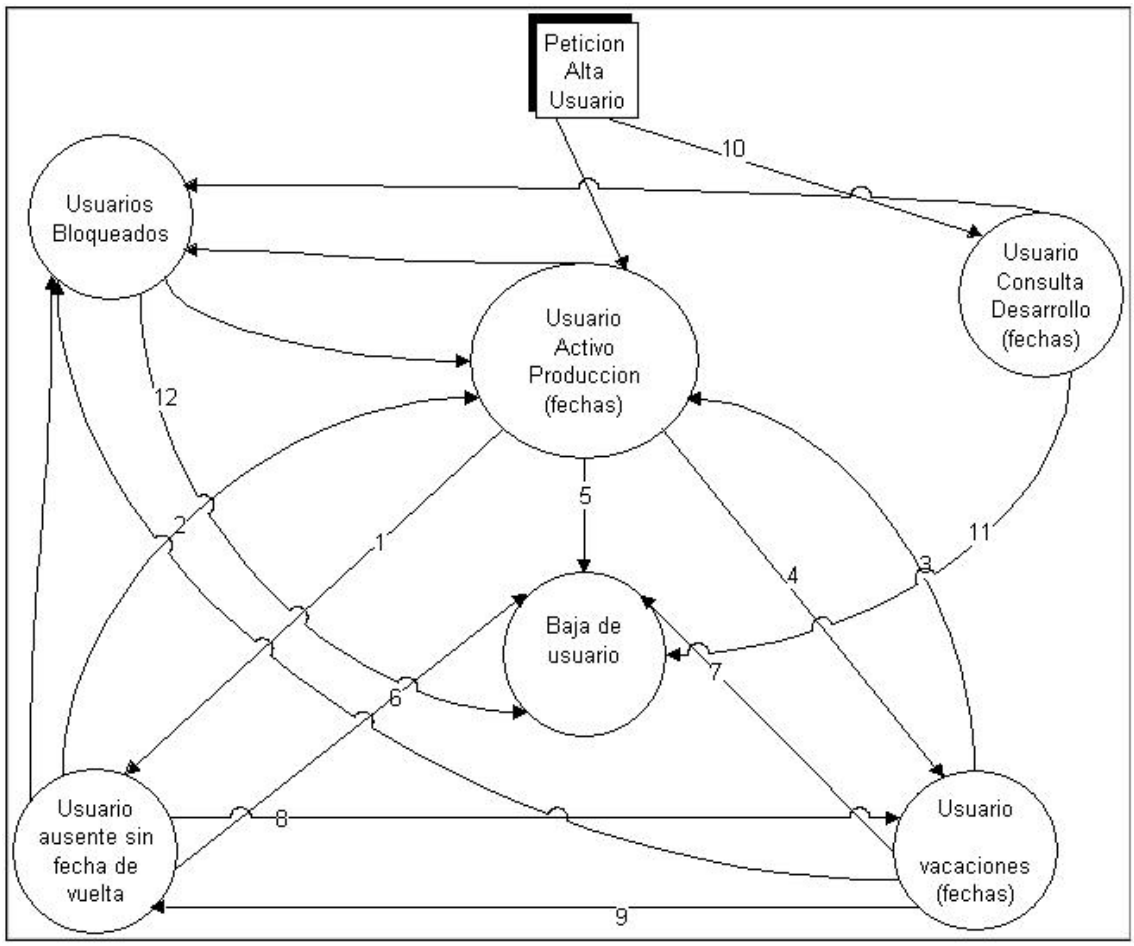
Desde el momento en que se crea un usuario, puede pasar por diferentes estados:

- Activo entre fechas (el usuario puede iniciar sesión entre las fechas indicadas).
- Bloqueado (por inactividad, por exceso de reintentos en el inicio de sesión…
- De vacaciones (con fecha de inicio y fin de vacaciones=.

- Ausente sin fecha de vuelta (el usuario no podrá iniciar sesión y, además, quedará exento del proceso automático de borrado de usuarios).
- De baja (el usuario no podrá iniciar sesión y también quedará exento del proceso de borrado).

Los cambios que se van produciendo en un perfil de usuario se reflejarán en un fichero de "log" donde se conservará información de la acción realizada y del día y la hora, así como el último inicio de sesión del usuario y el último cambio de clave.

La relación entre los cambios de estados que pueden producirse son:

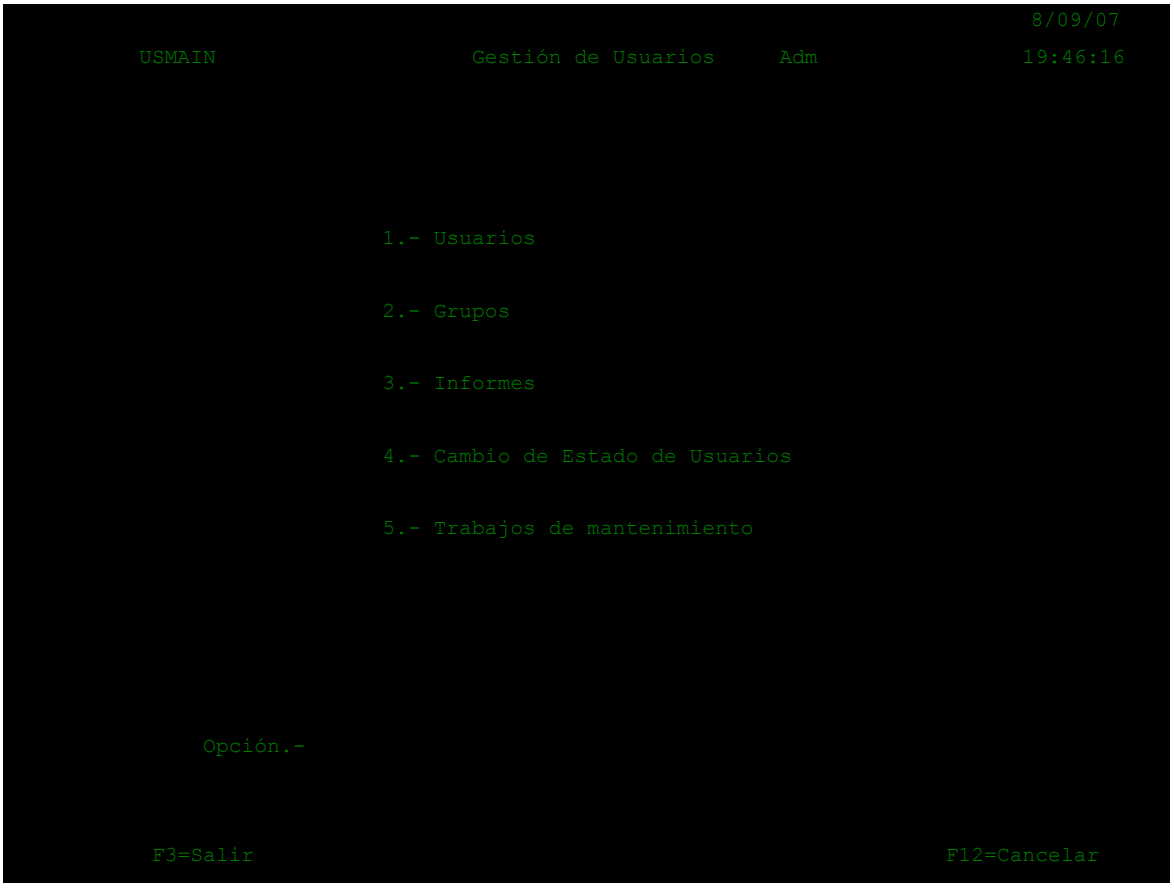


3.3.3. Manual de uso

Pantalla principal

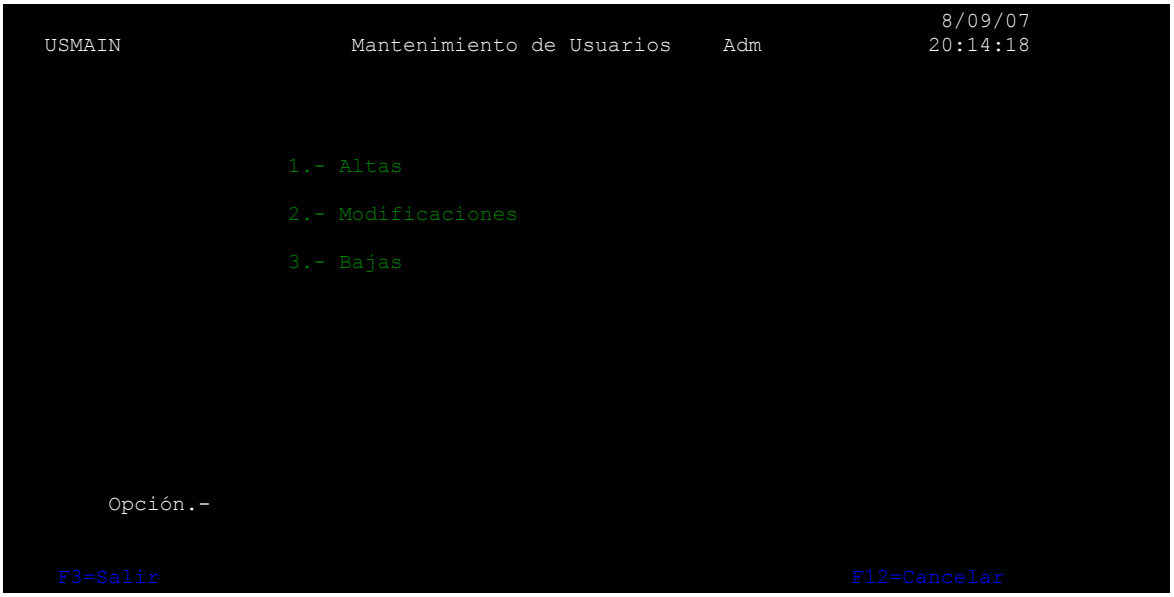
Desde la pantalla principal de la aplicación podemos acceder a la gestión de usuarios, la de grupos, la generación de informes, al cambio de estado de un usuario y al lanzamiento manual del proceso “batch” de mantenimiento de usuarios.

A pesar de que el cambio de estado de usuarios debería estar englobado en el apartado de usuarios, dada la alta frecuencia con la que se utiliza se ha puesto en la pantalla principal, de esta forma se mejora el acceso y se agilizan estas tareas que son las más utilizadas.



Opción 1

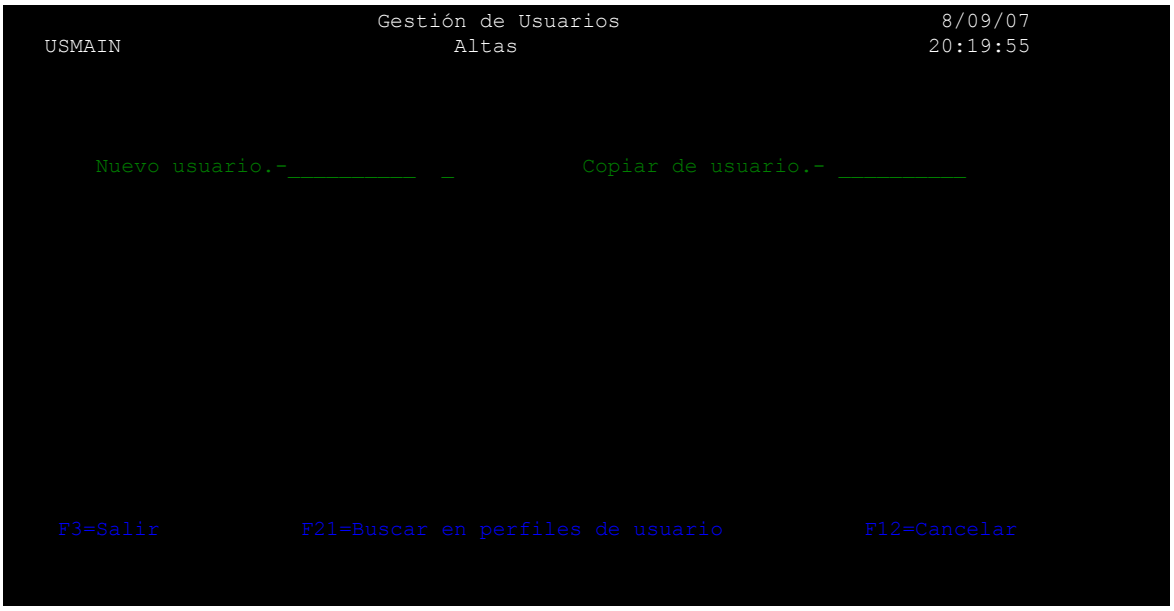
Dentro del apartado de usuarios, podemos dar de alta un usuario, modificar sus características o darlo de baja.



Opción 1.1

Al dar de alta un usuario se puede hacerlo a partir de un usuario nuevo o como copia de uno existente. Si escribimos las primeras letras de un usuario (las correspondientes al grupo al que pertenece) y ponemos un signo + en la casilla que hay a continuación, el sistema pondrá en el campo “Copiar de usuario” el primer usuario (por orden alfabético) que comience con las mismas iniciales que le hemos indicado en el campo “Nuevo usuario”.

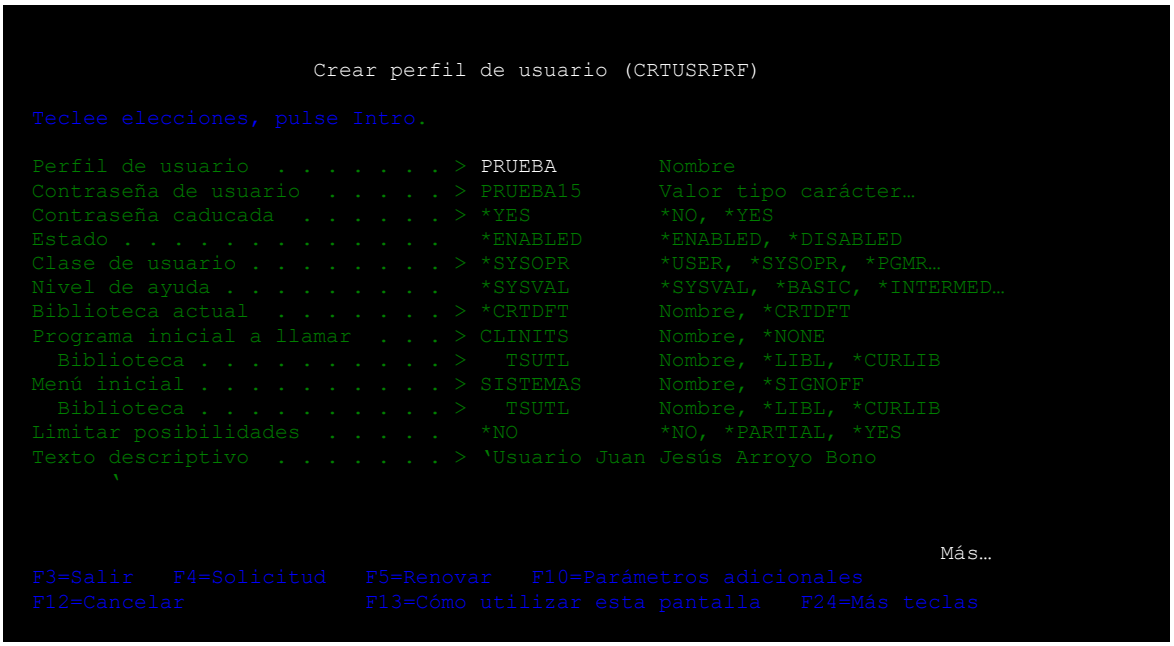
Presionando la tecla F21, se realiza una búsqueda en el sistema de aquellos usuarios que ya existan pero que no estén dados de alta en la aplicación de usuarios. Estos usuarios serán insertados automáticamente en los ficheros de la aplicación.



Tanto si se crea un usuario nuevo, como si se copia de otro existente, la aplicación nos solicitará el código de la Solicitud de Mantenimiento que ha solicitado el alta del usuario para anotarla en el histórico.

Posteriormente, aparecerán los parámetros que el sistema solicita al crear un perfil de usuario, en caso de haberse indicado un usuario de copia, dichos campos aparecerán con la información del usuario original, en caso contrario, aparecerán con los valores por defecto del sistema.

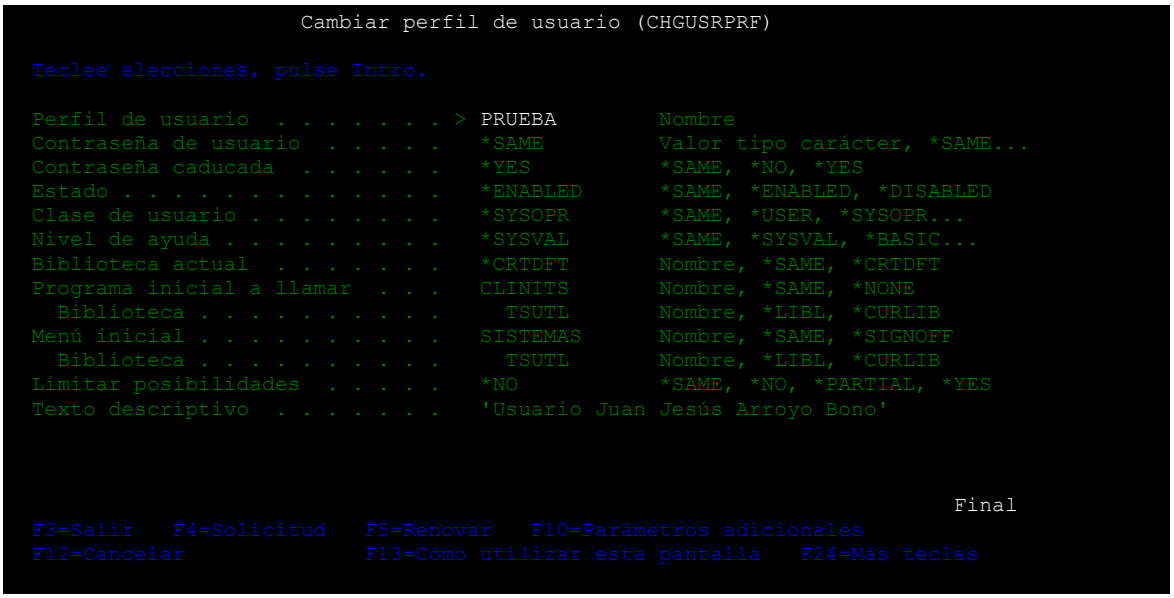
La aplicación rellenará automáticamente el campo contraseña del usuario con una clave generada aleatoriamente.



Opción 1.2

Todos las propiedades de un perfil de usuario se pueden modificar desde esta opción, de este modo quedarán registrados en los ficheros de la aplicación.

Los campos a modificar son los mismos que cuando se crea un usuario.



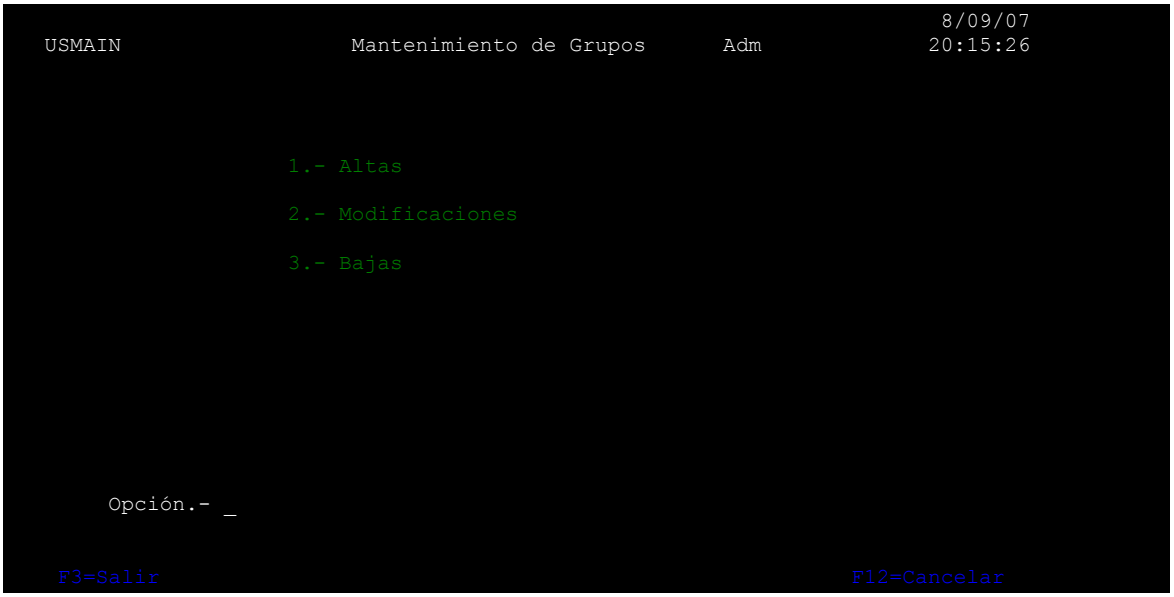
Opción 1.3

También permite borrar un usuario, eliminándolo de la aplicación de usuarios.

Para el borrado de un usuario también será necesario indicar el código de la Solicitud de Mantenimiento que solicita el borrado.

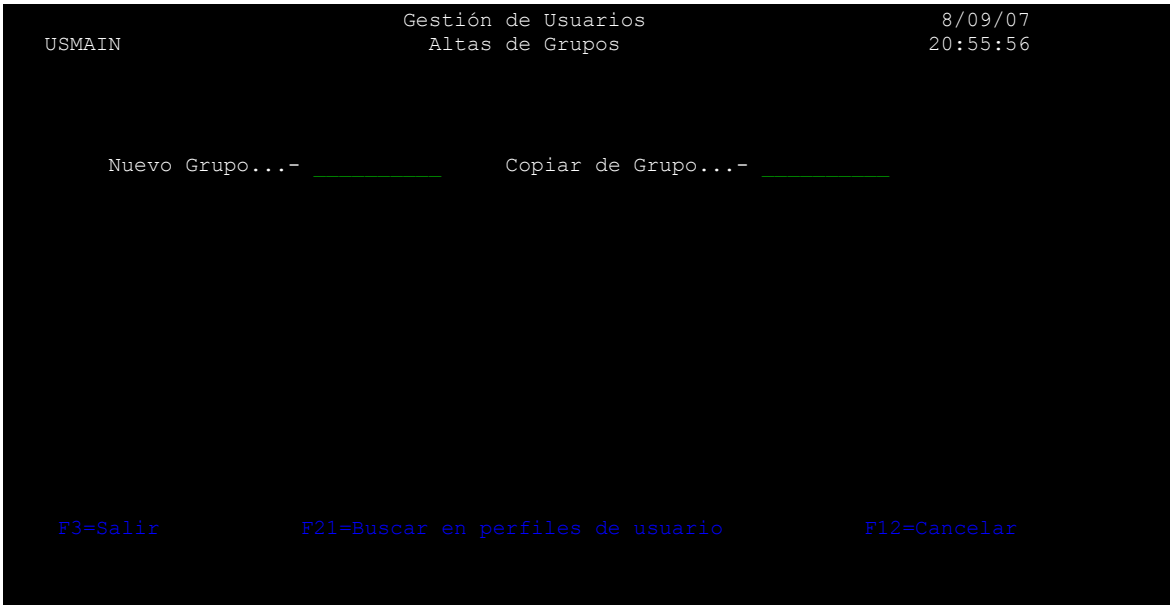
Opción 2

Con los grupos se podrán realizar las mismas tareas que las realizadas con los usuarios, altas, modificaciones y bajas.



Opción 2.1

La aplicación permite crear un grupo a imagen de otro ya existente.

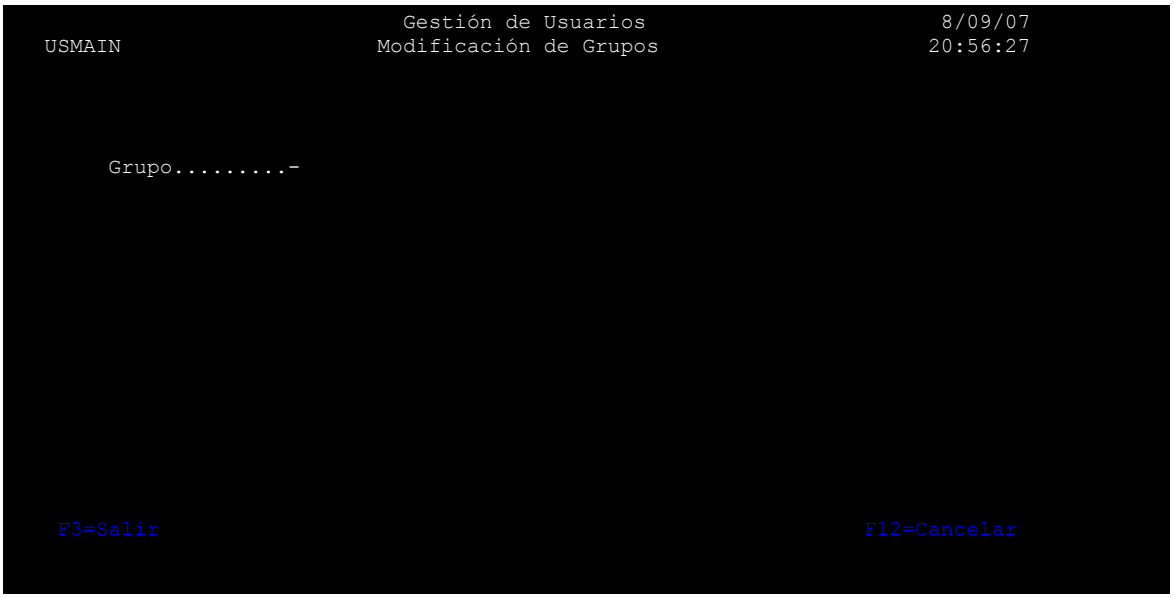


En el AS400 los parámetros de un grupo son los mismos que los de un usuario, de hecho el objeto creado pertenece al mismo tipo “*USRPRF”.

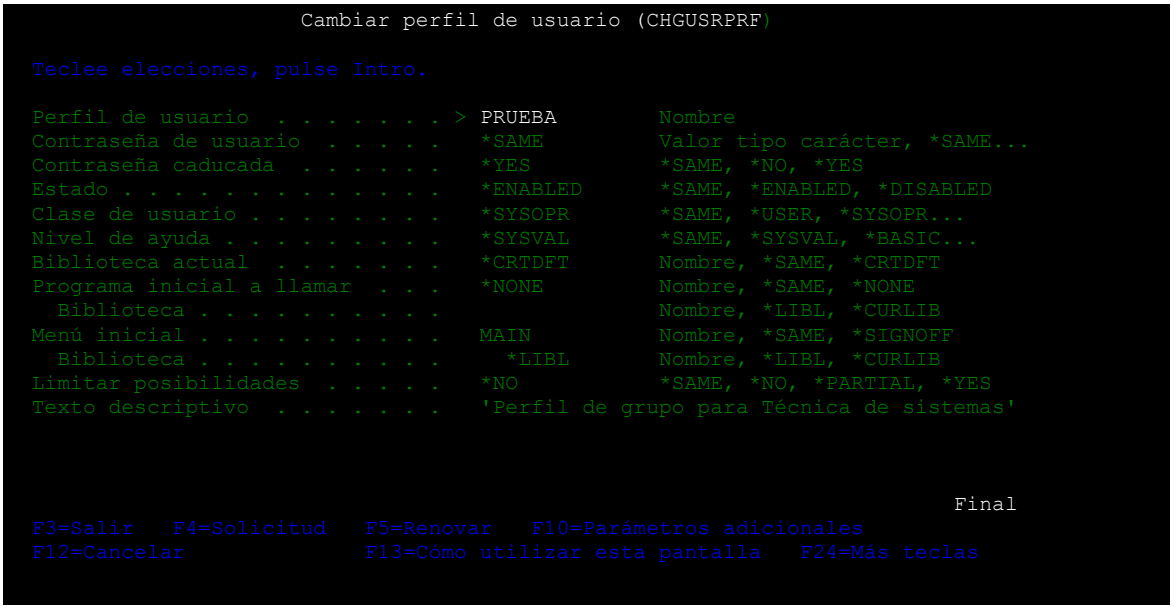
En este caso, como los grupos no inician sesión, se indicará que la clave del usuario es “*NONE”, que el estado es “*DISABLED” y que el menú inicial es “*SIGNOFF”. De este modo evitaremos (por triplicado) que ningún usuario pueda iniciar sesión con el identificador de un grupo.

Opción 2.2

Todos los parámetros que definen un grupo podrán ser modificados desde esta opción.



Los parámetros corresponden a los que el sistema asigna a los perfiles.



Opción 2.3

Al borrar un grupo también deberemos indicar el motivo del borrado. A diferencia del borrado de usuarios, en el de grupos no se solicita el código de la Solicitud de Mantenimiento, dado que las causas pueden ser muy diferentes, sin embargo se permite escribir el motivo del borrado para que quede anotado en la aplicación.

Opción 3

Se requiere que la aplicación genere una serie de informes, diferentes según las necesidades de los diferentes usuarios que van a utilizar la aplicación. Los informes corresponden a los usuarios del sistema, los grupos y al registro de acciones realizadas por la aplicación.

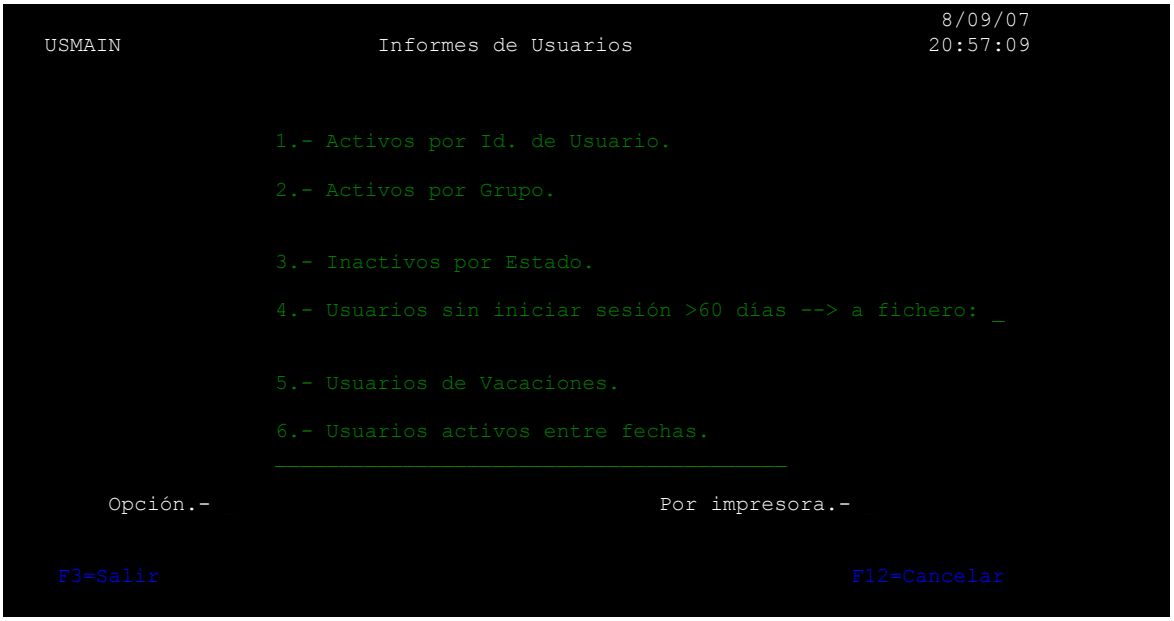
Opción 3.1

Por defecto los informes se muestran por pantalla, pero, marcando una S en el campo “Por impresora” se generará el informe en la salida de impresión del usuario y, posteriormente, este informe se podrá enviar a una impresora del sistema.

En el apartado de usuarios se pueden obtener distintos tipos de informes:

1. Usuarios activos, ordenados por su identificador.
2. Usuarios activos, ordenados por el grupo al que pertenecen.
3. Usuarios inactivos, ordenados por el estado en el que se encuentran.
4. Usuarios que no han iniciado sesión hace más de 60 dias.
5. Usuarios de vacaciones.
6. Usuarios activos, indicando entre que fechas permanecerán activos.

El proceso “batch” de la aplicación de usuarios genera un objeto con el listado de los usuarios que no han iniciado sesión en más de 60 días, esta información se envía periódicamente a la Oficina de Proyectos para que soliciten, si es necesario, la baja (o el cambio de estado) de los usuarios. Si fuese necesario se puede generar manualmente esta información (sin necesidad de lanzar el proceso “batch” indicando una S en el campo “A fichero” y generando el informe.



Opción 3.1.1

En esta opción se genera un listado de los usuarios activos, indicando el nombre del usuario, el grupo al que pertenecen y su descripción (que deberá indicar el nombre y apellidos del usuario al que pertenece el perfil).

Finalmente indicará el total de usuarios que están activos en este sistema.

```
                          Visualizar Informe
Consulta. . :   TSAPUSU/USINFQRY01          Ancho informe. . . . . :      82
Situar en línea  . . . . . .              Desplaz. a columna . . . . . .
Fila   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7..
             Usuario     Grupo       Descripción
             ----------  ----------  --------------------
000061       TSI001      TSISTEMAS   Perfil de Juan Jesús Arroyo Bono
000062       TSI002      TSISTEMAS   Perfil de Usuario 2
000063       TSI003      TSISTEMAS   Perfil de Usuario 3
000064       TSI004      TSISTEMAS   Perfil de Usuario 4
000065       TSI006      TSISTEMAS   Perfil de Usuario 6
000066       TSI009      TSISTEMAS   Perfil de Usuario 9
000067       TSI010      TSISTEMAS   Perfil de Usuario 10
000068       TSI011      TSISTEMAS   Perfil de Usuario 11
000069       TSI012      TSISTEMAS   Perfil de Usuario 12
000070       TSI015      TSISTEMAS   Perfil de Usuario 15
000071       TSI017      TSISTEMAS   Perfil de Usuario 17
000072
000073 Total Usuarios.-
000074 CUENTA 71
****** ********  Fin de informe  ********
                                                                      Final
F3=Salir  F12=Cancelar    F19=Izquierda    F20=Derecha    F21=Dividir
```

Opción 3.1.2

En esta opción se muestran los usuarios activos ordenados por grupos, se muestra el grupo del usuario, su identificador y su descripción.

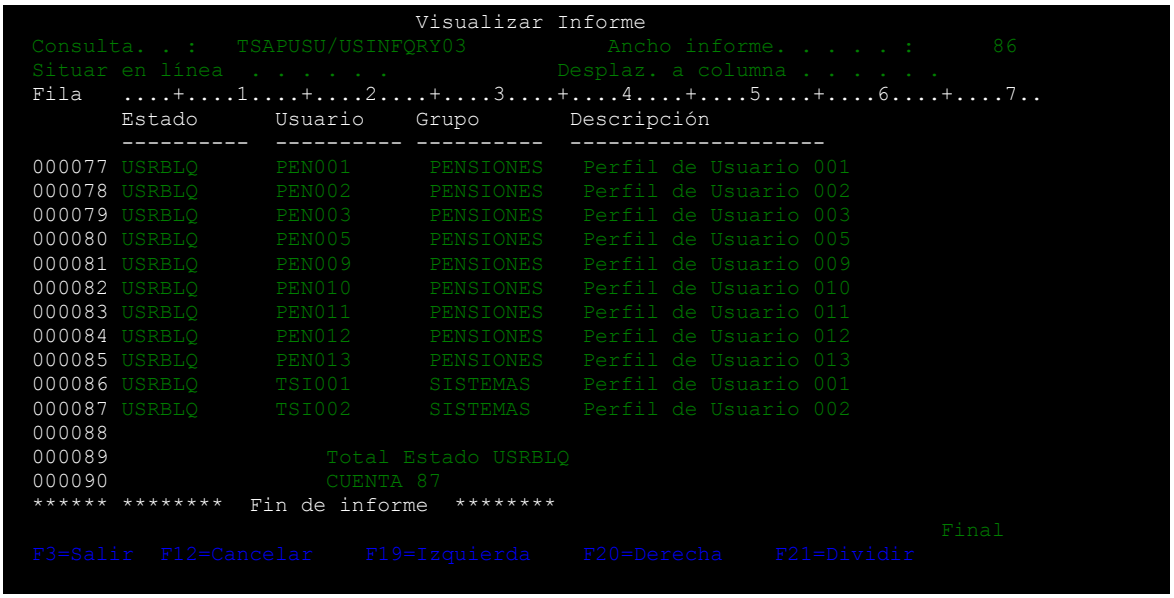
También se mostrará el número de usuarios que pertenecen a un grupo.

```
                          Visualizar Informe
Consulta. . :   TSAPUSU/USINFQRY02          Ancho informe. . . . . :      83
Situar en línea  . . . . . .              Desplaz. a columna . . . . . .
Fila   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7..
             Grupo       Usuario     Descripción
             ----------  ----------  --------------------
000016       SEGUROS     SEG001      Perfil de usuario 001
000017       SEGUROS     SEG002      Perfil de usuario 002
000018       SEGUROS     SEG003      Perfil de usuario 003
000019       SEGUROS     SEG004      Perfil de usuario 004
000020       SEGUROS     SEG005      Perfil de usuario 005
000021
000022  Total Grupo SEGUROS
000023  CUENTA 20
000024
000025       CONSULTA    CON001       Perfil de Usuario 001
000026
000027  Total Grupo CONSULTA
000028  CUENTA 1
000029
000030       CONTAB      COB001       Perfil de usuario 001
                                                                      Más...
F3=Salir  F12=Cancelar    F19=Izquierda    F20=Derecha    F21=Dividir
```

Opción 3.1.3

Con esta opción se muestran los usuarios inactivos del sistema, ordenados por el estado (bloqueado, ausente, de vacaciones o de baja).

Se muestra el total de usuarios que permanecen en los diferentes estados.

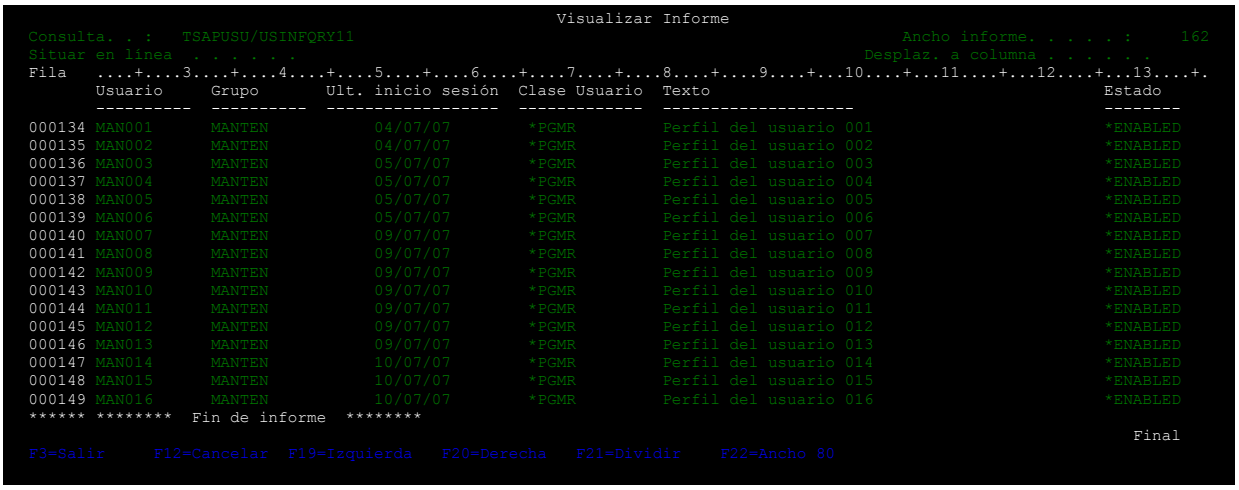


```
                          Visualizar Informe
Consulta. . :   TSAPUSU/USINFQRY03          Ancho informe. . . . . :      86
Situar en línea  . . . . . .              Desplaz. a columna . . . . . .
Fila   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7..
       Estado      Usuario    Grupo       Descripción
       ----------  ---------- ----------  --------------------
000077 USRBLQ      PEN001      PENSIONES   Perfil de Usuario 001
000078 USRBLQ      PEN002      PENSIONES   Perfil de Usuario 002
000079 USRBLQ      PEN003      PENSIONES   Perfil de Usuario 003
000080 USRBLQ      PEN005      PENSIONES   Perfil de Usuario 005
000081 USRBLQ      PEN009      PENSIONES   Perfil de Usuario 009
000082 USRBLQ      PEN010      PENSIONES   Perfil de Usuario 010
000083 USRBLQ      PEN011      PENSIONES   Perfil de Usuario 011
000084 USRBLQ      PEN012      PENSIONES   Perfil de Usuario 012
000085 USRBLQ      PEN013      PENSIONES   Perfil de Usuario 013
000086 USRBLQ      TSI001      SISTEMAS    Perfil de Usuario 001
000087 USRBLQ      TSI002      SISTEMAS    Perfil de Usuario 002
000088
000089                 Total Estado USRBLQ
000090                 CUENTA 87
****** ********  Fin de informe  ********
                                                                    Final
F3=Salir  F12=Cancelar    F19=Izquierda    F20=Derecha    F21=Dividir
```

Opción 3.1.4

No es habitual que un usuario permanezca más de 60 días sin iniciar sesión, por lo que estos casos deben ser estudiados por la Oficina de Proyectos para pasar los usuario de estado activo al estado correspondiente con la situación del usuario.

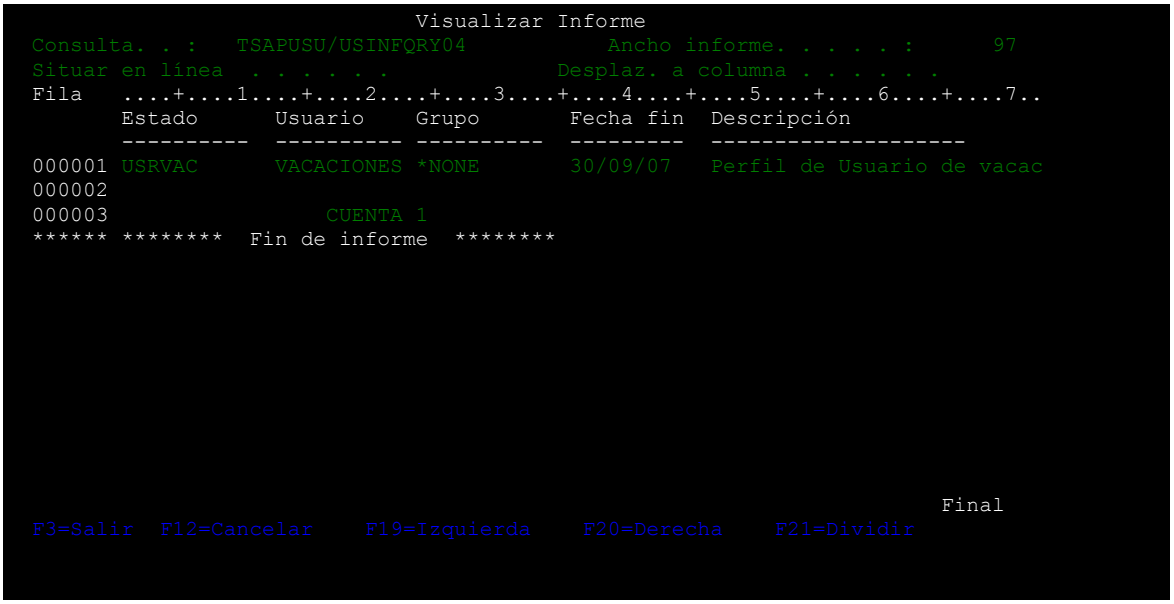
Este informe se envía periódicamente y muestra el identificador de usuario, el grupo al que pertenece, cuando realizó su último inicio de sesíon, qué tipo de usuario es, su descripción y el estado actual del usuario.



Opción 3.1.5

Este informe muestra todos los usuarios que actualmente están de vacaciones. Los datos que se muestran son el estado, el identificador del usuario, el grupo al que pertenece, la fecha de finalización de sus vacaciones y la descripción del usuario.

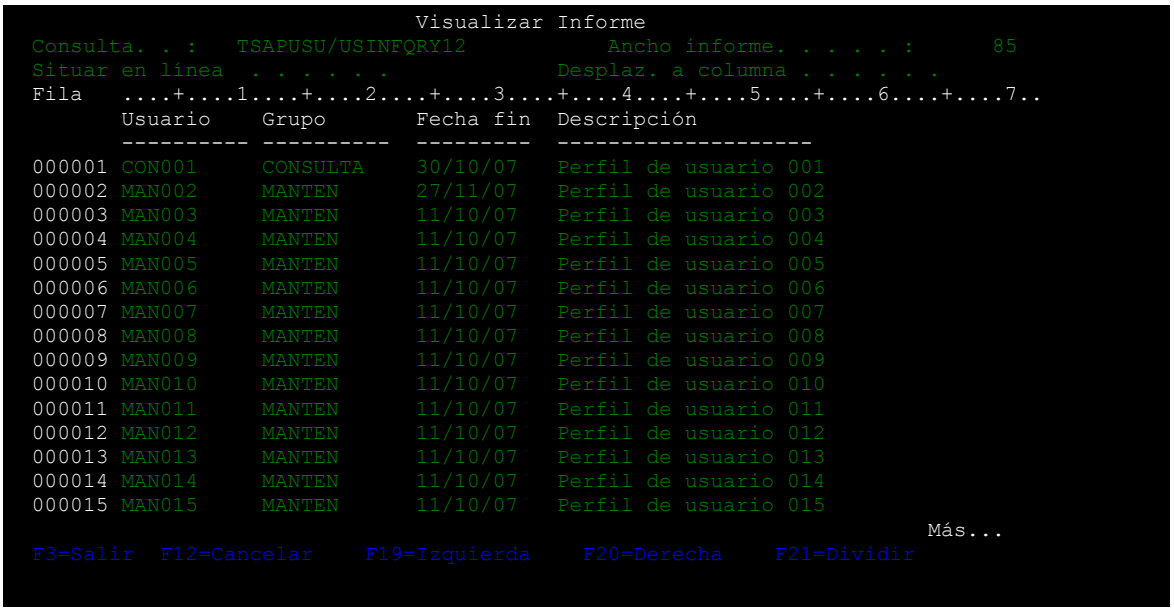
También se muestra el total de los usuarios que están en este estado.



Opción 3.1.6

En este informe se muestran los diferentes usuarios activos del sistema que están activos entre fechas.

Se muestra el identificador del usuario, el grupo al que pertenece, la feche de fin de activación y la descripción del usuario.



```
                          Visualizar Informe
Consulta. . :   TSAPUSU/USINFQRY12          Ancho informe. . . . . :      85
Situar en línea  . . . . . .              Desplaz. a columna . . . . . .
Fila   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7..
       Usuario    Grupo       Fecha fin  Descripción
       ---------- ----------  ---------  --------------------
000001 CON001     CONSULTA    30/10/07   Perfil de usuario 001
000002 MAN002     MANTEN      27/11/07   Perfil de usuario 002
000003 MAN003     MANTEN      11/10/07   Perfil de usuario 003
000004 MAN004     MANTEN      11/10/07   Perfil de usuario 004
000005 MAN005     MANTEN      11/10/07   Perfil de usuario 005
000006 MAN006     MANTEN      11/10/07   Perfil de usuario 006
000007 MAN007     MANTEN      11/10/07   Perfil de usuario 007
000008 MAN008     MANTEN      11/10/07   Perfil de usuario 008
000009 MAN009     MANTEN      11/10/07   Perfil de usuario 009
000010 MAN010     MANTEN      11/10/07   Perfil de usuario 010
000011 MAN011     MANTEN      11/10/07   Perfil de usuario 011
000012 MAN012     MANTEN      11/10/07   Perfil de usuario 012
000013 MAN013     MANTEN      11/10/07   Perfil de usuario 013
000014 MAN014     MANTEN      11/10/07   Perfil de usuario 014
000015 MAN015     MANTEN      11/10/07   Perfil de usuario 015
                                                            Más...
F3=Salir  F12=Cancelar    F19=Izquierda    F20=Derecha    F21=Dividir
```

Opción 3.2

Se pueden visualizar todas las acciones realizadas con la aplicación de usuarios.

Los campos mostrados son:

- Usuario al que afecta la acción.
- Fecha en que se realiza.
- Hora de la acción.
- Acción realizada sobre el usuario. Existen diferentes tipos:
  - BLQ_PWD, bloqueo del usuario por exceso de intentos incorrectos de inicio de sesión.
  - BLQ_USR, bloqueo manual del usuario.
  - BOR_USR, borrado de un usuario.
  - CHG_GRP, cambio de grupo de un usuario.

- CRT_USR, alta de un usuario.
- DESBL_USR, desbloqueo de un usuario.
- INI_CONS, activación manual de un usuario.
- INI_VAC, desactivación de un usuario de vacaciones entre fechas.
- USR_FIN, finalización automática del estado, activo o inactivo, entre fechas.
- USR_INI, activación automática de un usuario entre fechas.

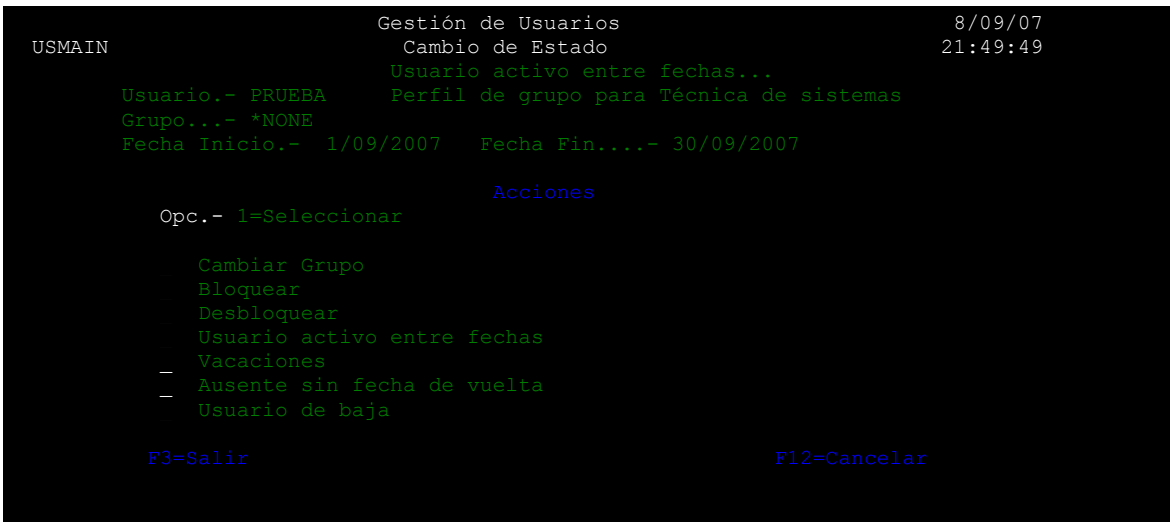
- Usuario que realiza la acción. Las acciones del usuario BATCH corresponden con las realizadas por el proceso “batch”.
- Solicitud de Mantenimiento, en caso de altas, bajas o desbloqueos de usuarios.
- Ultimo inicio de sesión del usuario, en caso de bloqueo automático del usuario.
- Ultimo cambio de clave, en caso de bloqueo automático del usuario.
- Intentos incorrectos de inicio de sesión realizados por el usuario.
- Bloqueo por exceso de intentos de inicio de sesión, como motivo en caso de un desbloqueo de usuario.
- Bloqueo por inactividad del usuario, como motivo en caso de un desbloqueo de usuario.

```
                                        Visualizar Informe
 Consulta. . :   TSAPUSU/USINFQRY10                                    Ancho informe. . . . . :
120
 Situar en línea  . . . . . .  B                                      Desplaz. a columna . . . . . .
 Fila   ....+....1....+....2....+....3....+....4....+....5....+....6....+....7....+....8....+....9....+...10....+...11....+...12
                                                                                                 Bloqueo    Bloqueo
       Usuario     Fecha    Hora     Acción      Usr. Acción  Sol. Mtto. U.Ini. Ses. U.Cam. Pwd. Pwd Inc   contrasñ.  tiempo
       ----------  -------- -------- ----------  -----------  ---------- ----------- ----------- -------   ---------  ---------
 003427
 003428 TSSI002     07/07/07 06:30:36 BLQ_PWD     BATCH                     070705      070507          5
 003429
 003430 CON001      09/07/07 06:30:38 BLQ_USR     BATCH                     070509      070509          0
 003431
 003432 MAN001      11/07/07 06:30:29 BLQ_USR     BATCH                     070511      070509          0
 003433
 003434 COB001      12/07/07 12:49:39 DESBL_USR   TSI001        CP12345-07                            0                    X
 003435
 003436 PRUEBA      08/09/07 21:20:04 CRT_USR     TSI001        PRUEBA                                0
 003437 PRUEBA      08/09/07 21:24:34 BOR_USR     TSI002        PRUEBA                                0
 003438 PRUEBA      08/09/07 21:29:27 CRT_USR     TSI001                                              0
 003439 PRUEBA      08/09/07 21:46:50 INI_VAC     TSI001                                              0
 003440 PRUEBA      08/09/07 21:49:45 INI_CONS    TSI001                                              0
 003441 PRUEBA      08/09/07 21:53:09 BLQ_USR     TSI001                                              0
 003442 PRUEBA      08/09/07 21:53:24 BLQ_USR     TSI001                                              0
 ****** ********  Fin de informe  ********
                                                                                                                      Final
 F3=Salir     F12=Cancelar  F19=Izquierda   F20=Derecha   F21=Dividir    F22=Ancho 80
```

Opción 4

Una gran cantidad de las acciones que se realizan en la aplicación de usuarios corresponde a un cambio de estado de los usuarios.

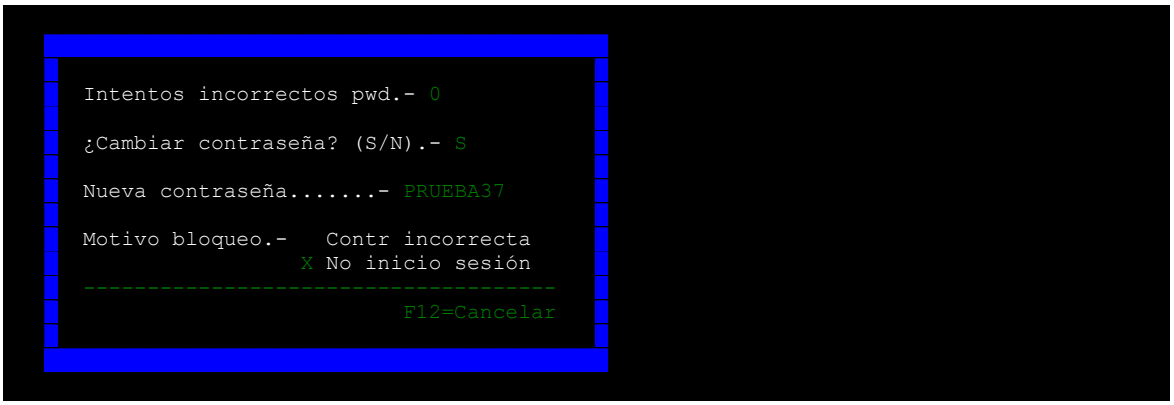
Tras indicar el usuario sobre el que queremos realizar la acción, aparecerán las opciones que se permiten.



Estos cambios de estado pueden ser de tipo:

- Cambio de grupo. Se deberá indicar el grupo al que se quiere asignar el usuario.

- Bloqueo manual del usuario. El usuario cambiará al estado de usuarios bloqueados.
- Desbloqueo del usuario. Se mostrarán el número de intentos incorrectos de inicio de sesión que ha realizado el usuario. Se nos preguntará si se desea cambiar la clave del usuario y en caso afirmativo, se nos creará una clave aleatoria. El sistema marcará la casilla correspondiente en caso de que el usuario se haya bloqueado por exceso de intentos o por no haber iniciado sesión.



Este cambio de estado debe ser pedido mediante una Solicitud de Mantenimiento, la aplicación nos solicitará su código.

- Asignación de fechas entre las que está activo un usuario.

Se puede indicar entre qué fechas se debe mantener activo un usuario, al finalizar el periodo el usuario será bloqueado automáticamente.

```
                                          DDMMAAAA
Usuario activo entre fechas ---->|Fecha inicio: 01092007
                                 |Fecha fin...: 30092007
```

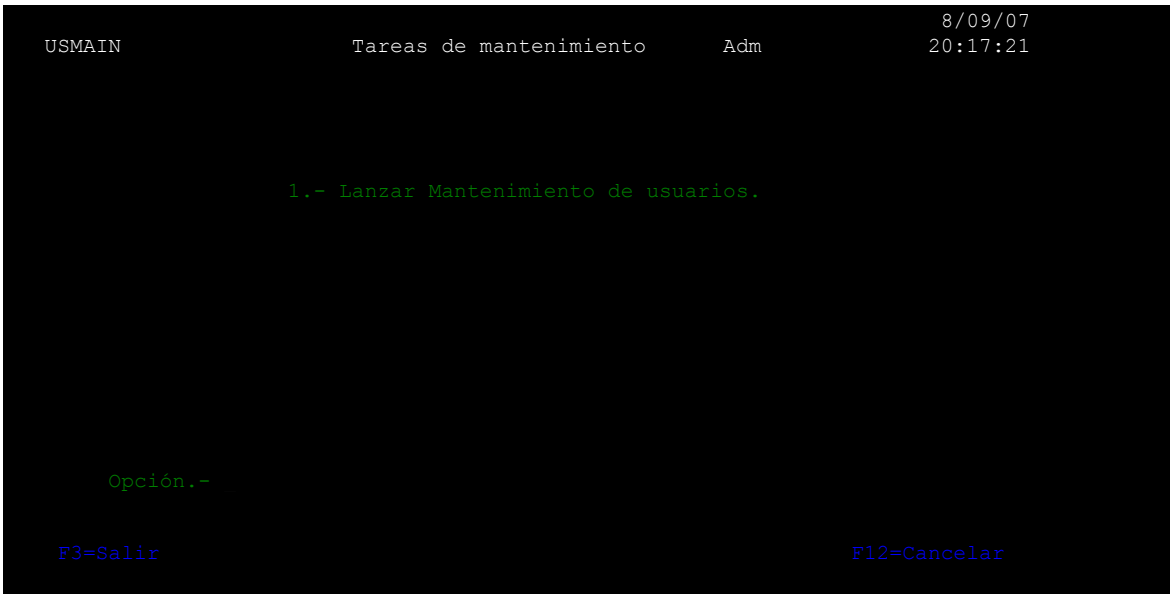
- Cambio a estado vacaciones de un usuario, indicando las fechas de inicio y fin. El día en el que se inicien las vacaciones, el usuario pasará a estado inactivo y quedará excluido de los procesos de mantenimiento de la aplicación de usuarios. El usuario será activado automáticamente el dia del fin de sus vacaciones.

```
                                          DDMMAAAA
                                 |Fecha inicio: 01092007
Vacaciones ---------------------->|Fecha fin...: 30092007
```

- Cambio a estado ausente sin fecha de vuelta de un usuario. Este estado es equiparable al estado de vacaciones con la diferencia de que al no existir fecha de vuelta la activación deberá ser manual.
- Cambio a estada de baja. En este estado el usuario pasará a estado inactivo. Con las mismas características que el estado anterior, se ha diferenciado a efectos organizativos.

Opción 5

El proceso “batch” de mantenimiento de usuarios se lanzará diariamente por el planificador del sistema (WRKJOBSCDE) a una hora de bajo impacto en el sistema (6:30 AM). También se permite el lanzamiento manual del proceso.



Antes de ejecutarse, se pide una confirmación.

3.3.4. Proceso “batch”

La aplicación de usuarios consta también de una parte “batch” que es la encargada de realizar el mantenimiento de los usuarios.

Por una parte se encarga de bloquear aquellos usuarios que llevan más de 30 días inactivos (entendiendo por actividad el haber iniciado una sesión en la máquina), la permanencia de estos usuarios en estado activo puede representar un problema para la seguridad, pues, la mayoría de veces, se trata de usuarios que ya no son necesario y que nadie ha notificado este cambio a la Oficina de Proyectos.

Posteriormente, también se genera un listado de los usuarios que no han iniciado sesión en 90 días para que la Oficina de Proyectos estudie la situación de los usuarios y tome una decisión respecto a su borrado o su cambio a un estado distinto (que puede ser Baja o Vacaciones).

También se actualizan los ficheros de las bases de datos de la aplicación con la información de los excesos de reintentos de los usuarios, esta información será mostrada en la pantalla de desbloquear un usuario para facilitar la elección del motivo de bloqueo (por exceso de reintentos o por inactividad).

En aquellos usuarios que se ha indicado que están activos entre fechas, el proceso debe consultar si la fecha actual coincide con su fecha de inicio, y, en caso afirmativo, debe proceder a su activación. Así mismo debe comprobar las fechas de finalización de todos los usuarios para proceder a su desactivación, si es necesario.

Del mismo modo, para los usuarios con fecha de vacaciones, deberá comprobar si se está entre estas fechas para mantenerlo en el estado Vacaciones o devolverlo al estado de Activo.

Todas estas tareas generarán sus respectivos informes que serán enviados a los diferentes departamentos para que los revisen y tomen las medidas adecuadas en cada uno de los casos.

3.4. Otras recomendaciones

3.4.1. Poner PWD a *NONE de grupos SEGUROS y PENSIONES

Se cambia la clave de los perfiles de usuarios SEGUROS y PENSIONES a *NONE, de este modo se evitan los inicios de sesión de estos perfiles que están creados únicamente para que realicen labor de agrupar a los usuarios.

3.4.2. Poner CURLIB en TSISTEMAS, EXPLO e INSTAL

La biblioteca indicada en este parámetro será la primera en la que se busquen los objetos y programas ejecutados por el usuario, para evitar posibles problemas en la ejecución de programas se definen varias bibliotecas para cada tipo de usuario. TSUTL para el grupo TSISTEMAS, EXPLOT para el grupo EXPLO y MANTEN para el grupo INSTAL. Además, los usuarios que no tienen biblioteca asignada en el parámetro CURLIB, por defecto crean los objetos en la que asigna el sistema QGPL, esto causa que se creen, por error, los objetos en dicha biblioteca, objetos que a posteriori pueden interferir en el trabajo de otros usuarios.

3.4.3. Crear JOBD para INSTALL, TSISTEMAS y EXPLO

Una descripción de trabajo (JOBD) indica con qué características se ejecutarán los procesos que lanza el usuario (colas de salida, subsistemas, prioridades, etc.). El sistema por defecto asigna la descripción de trabajo QDFTJOBD a aquellos usuarios que no tienen indicada ninguna en el perfil de usuario. Si se crea una a cada grupo de usuarios se evitará que cualquier cambio concreto que afecte a un grupo se replique involuntariamente en el resto de los grupos. También permitirá, creando nuevas colas de trabajo, que cada grupo lance sus trabajos por una distinta de modo que se puedan gestionar separadamente.

3.4.4. Añadir *CMD a la auditoria de SEGUROS y PENSIONES

Desde el punto de vista de la seguridad, el añadir al registro de diario todos los comandos que lancen los usuarios de SEGUROS y PENSIONES, aumentará sensiblemente la seguridad. Pero dichas anotaciones aumentarán en gran medida el tamaño de los receptores, no existiendo actualmente capacidad suficiente para soportarlo. Además estos grupos tienen sus acciones limitadas a las que se permiten por los menús de las aplicaciones que utilizan y no disponen de línea de comandos, por lo que el peligro que suponen para la seguridad del sistema es mínimo. También hay que tener en cuenta que existe un listado de ficheros definidos de importancia alta, que tienen registrados todos los accesos que se realicen, independientemente del grupo de usuarios al que se pertenezca.

3.4.5. Auditar todos los objetos del sistema

La situación ideal del sistema sería mantener registro de todas aquellas modificaciones que se realicen en cualquier objeto de datos del sistema. Esta situación se enfrenta a la imposibilidad que presenta por restricciones en el espacio disponible en disco, además de la merma de rendimiento del sistema que esto supondría. En la actualidad existe un listado de objetos de datos definidos como importantes en el sistema que están registrados por diario existiendo un procedimiento por el cual, cuando se va a crear uno nuevo considerado de importancia alta, se añade a su respectivo diario.

3.4.6. Revisar usuarios fuera de nomenclatura

Tras revisar cuidadosamente los usuarios que no siguen la nomenclatura correcta, se cambian los usuarios al grupo de TSISTEMAS.

3.4.7. Unificar usuarios de seguros y pensiones

Se estudian y definen las características que deben tener los usuarios de los grupos de SEGUROS y PENSIONES.

Se cambian todos los perfiles para que tengan las propiedades que les corresponden según el grupo al que pertenecen.

4. Seguridad de recursos

4.1. Introducción

Tras el informe de los excesivos fallos en la seguridad que presenta el sistema, y a pesar del esfuerzo que esto va a suponer, se toma la decisión de definir una política de seguridad partiendo desde cero, de este modo se evitarán errores que se han venido arrastrando desde los inicios del sistema.

Se deberá llegar a un consenso entre las partes implicadas de cuales son las necesidades reales de los usuarios y cómo se verán reflejadas dichas necesidades en el sistema.

Al mismo tiempo, y aunque no es nuestro objetivo, se obtendrá un documento en el que se “normalizará” el modo de trabajo de los diferentes grupos de usuarios y se detectarán aquellas acciones “irregulares” que se deberían evitar o, cuanto menos, identificar como potencialmente peligrosas.

4.2. Análisis

En líneas generales se han tomado las siguientes directrices

- Para homogeneizar la asignación de permisos, se creará un grupo de usuarios por cada departamento, de modo que la asignación de permisos a los objetos se realizará directamente sobre este grupo.
- Cada grupo ejecutará sus trabajos “batch” sobre una cola de salida diferente, estas colas de salida estarán limitadas a un máximo de un trabajo activo, de este modo se evita que ningún grupo interfiera en el trabajo de los demás ocupando todo el subsistema o consumiendo excesivos recursos de la máquina.
- Para asignar una cola a un grupo de usuarios, se creará una descripción de trabajo para cada grupo.
- El propietario de los objetos será el grupo al que pertenece el usuario, se evita que durante el trabajo habitual un usuario cree objetos que no puedan ser accedidos por sus compañeros.
- Para evitar que se utilice como biblioteca actual (CURLIB) la biblioteca del sistema, se asignará a cada grupo una biblioteca propia diferente. De este modo se consigue, además, minimizar la interferencia que se pueda producir en la creación de objetos entre los distintos grupos.
- Se creará programas de inicio personalizados que cargarán las diferentes listas de bibliotecas que se considere necesarias para cada grupo. En este programa, además se comprobará que no se ha rebasado la cuota de ocupación del disco, generando un aviso en caso de haber sobrepasado el 80%. También se comprobará la fecha de fin de actividad del usuario y se enviará un mensaje en caso de que queden menos de 10 días.
- Todos los usuarios de un grupo tendrán auditados los mismos valores del sistema.

4.2.1. Departamento de Explotación

El usuario del departamento de explotación será de tipo *SYSOPR debido a que tiene implícito el *SAVSYS y el *JOBCTL, adicionalmente se modificarán las colas de salida que se consideren necesarias para que se puedan gestionar mediante el operador del sistema OPERCTL *YES.

El permisos *SAVSYS permite al usuario salvar, restaurar y liberar espacio de almacenamiento para todos los objetos del sistema, en los cuales el usuario tenga el permiso de existencia.

El permiso *JOBCTL permite al usuario las siguientes acciones:

- Cambiar, borrar, retener, liberar, visualizar, enviar y copiar todos los objetos en cualquier cola de salida que se especifique con el parámetro OPRCTL(*YES).
- Retener, liberar y eliminar colas de trabajo especificadas como OPRCTL(*YES).
- Retener, liberar y eliminar colas de salida especificadas como OPRCTL(*YES).
- Retener, liberar, cambiar y cancelar trabajos de usuario.
- Iniciar, cambiar, detener, retener y liberar, dispositivos de impresora, si en la cola de salida se ha especificado OPRCTL(*YES).
- Cambiar los atributos de ejecución de un trabajo, como pueden ser la impresora asociada, la prioridad del trabajo, etc.
- Parar subsistemas.
- Reiniciar la máquina (IPL “Inicial Program Load”).

El perfil del usuario tendrá los siguientes parámetros:

```
        Perfil usuario . . . . . :   EXPxxx
        Inicio sesión anterior . . . . . :   27/05/06  01:00:55
        Intentos inicio sesión no válidos  . . . . :   2
        Estado . . . . . :   *ENABLED
        Fecha último cambio contraseña . . . . . :   27/05/06
        Intervalo caducidad contraseña . . . . . :   *SYSVAL
          Fecha caducidad contraseña . . . . . :     26/07/06
        Establecer contraseña en caducada  . . . . :   *NO
        Gestión de la contraseña local . . . . . :   *YES
        Clase usuario  . . . . . :   *SYSOPR
        Autorizaciones especiales  . . . . . :   *JOBCTL
                                                 *SAVSYS
        Perfil grupo . . . . . :   EXPLO
        Propietario  . . . . . :   *GRPPRF
        Autorización grupo . . . . . :   *NONE
        Tipo de autorización de grupo  . . . . . :   *PRIVATE
        Grupos adicionales . . . . . :   *NONE
        Nivel de ayuda . . . . . :   *SYSVAL
        Biblioteca actual  . . . . . :   EXPLOT
        Programa inicial . . . . . :   CLINIEXP
          Biblioteca . . . . . :     TSUTL
        Menú inicial . . . . . :   EXPLOTP
          Biblioteca . . . . . :     TSUTL
        Limitar posibilidades  . . . . . :   *NO
        Texto  . . . . . :     Usuario de xxx
Visualizar información inicio sesión . . . :   *SYSVAL
        Limitar sesiones dispositivo . . . . . :   *SYSVAL
        Almacenamiento intermedio teclado  . . . . :   *SYSVAL
        Información de almacenamiento:
          Máximo almacenamiento permitido  . . . . :   *NOMAX
          Almacenamiento utilizado . . . . . :   32
          Almacenamiento utilizado en ASP
            independiente  . . . . . :   *NO
        Máxima prioridad planificación . . . . . :   3
        Descripción trabajo  . . . . . :   EXPJOBD
          Biblioteca . . . . . :     QUSRSYS
        Código contabilidad  . . . . . :
        Cola mensajes  . . . . . :   EXPxxx
          Biblioteca . . . . . :     QUSRSYS
        Entrega cola mensajes  . . . . . :   *NOTIFY
        Gravedad cola mensajes . . . . . :   00
        Cola salida  . . . . . :   *WRKSTN
          Biblioteca . . . . . :
        Dispositivo impresora  . . . . . :   *WRKSTN
        Entorno especial . . . . . :   *SYSVAL
        Programa de atención . . . . . :   *SYSVAL
          Biblioteca . . . . . :
        Secuencia de ordenación  . . . . . :   *SYSVAL
          Biblioteca . . . . . :
```

```
Identificador de idioma  . . . . . :   *SYSVAL
Identificador de país o región . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Opciones usuario . . . . . :   *NONE
Valor de auditoría de objeto . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
                                               *SYSMGT
Número de ID de usuario  . . . . . :   658
Número de ID de grupo  . . . . . :   *NONE
Directorio inicial . . . . . :   /home/EXPxxx
```

Los usuarios pertenecerán al grupo EXPLO, aquellos usuarios del departamento de explotación que sean jefes de turno tendrán como grupo secundario EXPLOTJT, esto permitirá restringir determinadas acciones solamente a estos últimos.

```
Grupos adicionales . . . . . :   EXPLOTJT
```

Gestión del Sistema

Como se ha comentado, el perfil *SYSOPR dispone de *SAVSYS y *JOBCTL por lo que la gestión habitual del sistema esta "asegurada".

Además este perfil de usuario puede realizar IPL, y otras tareas relacionadas con la gestión del sistema, definidas en el perfil de usuario *SYSOPR.

Las colas de salida que los operadores puedan visualizar estarán limitadas por la configuración del sistema. Concretamente tendrán permisos en las colas de trabajos SEGUROS, SEGUROST, PENSIONES y PENSIONEST.

El lanzamiento de trabajos en BATCH será posible, limitándose a la cola de trabajos EXPJOBQ, para ello se ha creado la descripción de trabajos EXPJOBD. Esta cola de trabajos se ha limitado a un máximo de 1 trabajo, pues se considera que no será necesaria la ejecución de más de un trabajo simultáneo.

Los parámetros de la descripción de trabajo EXPJOBD son:

```
Descripción trabajo:   EXPJOBD        Biblioteca:   QUSRSYS
Perfil usuario . . . . . . . . . . . . . . . . . :   *RQD
Comprobación sintaxis CL . . . . . . . . . . . . :   *NOCHK
Retener en cola de trabajos  . . . . . . . . . . :   *NO
Gravedad finalización  . . . . . . . . . . . . . :   30
Fecha trabajo  . . . . . . . . . . . . . . . . . :   *SYSVAL
Conmutadores trabajo . . . . . . . . . . . . . . :   00000000
Respuesta mensaje consulta . . . . . . . . . . . :   *RQD
Prioridad trabajo (en cola trabajos) . . . . . . :   5
Cola de trabajos . . . . . . . . . . . . . . . . :   EXPJOBQ
  Biblioteca . . . . . . . . . . . . . . . . . . :     QUSRSYS
Prioridad salida (en cola salida)  . . . . . . . :   5
Dispositivo impresora  . . . . . . . . . . . . . :   *USRPRF
Cola salida  . . . . . . . . . . . . . . . . . . :   *USRPRF
  Biblioteca . . . . . . . . . . . . . . . . . . :
Anotación mensajes:
  Nivel  . . . . . . . . . . . . . . . . . . . . :   4
  Gravedad . . . . . . . . . . . . . . . . . . . :   0
  Texto  . . . . . . . . . . . . . . . . . . . . :   *NOLIST
Anotar mandatos programa CL  . . . . . . . . . . :   *NO
Código contabilidad  . . . . . . . . . . . . . . :   *USRPRF
Texto impresión  . . . . . . . . . . . . . . . . :   *SYSVAL
Datos direccionamiento . . . . . . . . . . . . . :   QCMDI
Datos petición . . . . . . . . . . . . . . . . . :   *NONE
```

```
        Conversación de DDM  . . . . . :   *KEEP
        Acción recuperación dispositivo  . . . . . :   *SYSVAL
        Agrupación fin porción tiempo  . . . . . :   *SYSVAL
        Tamaño máximo de cola de mensajes del trabajo  . :   *SYSVAL
        Acción para cola de mensajes de trabajo llena  . :   *SYSVAL
        Permitir múltiples hebras  . . . . . :   *NO
        Grupo de ASP inicial . . . . . :   *NONE
        Acción de archivo en spool . . . . . :   *SYSVAL
        Texto  . . . . . :   Descripción de
trabajo usuarios Explotación
```

La cola EXPJOBQ ejecuta los trabajos en el subsistema QBATCH.

```
        Cola          Biblioteca     Trbjos     Subsistema     Estado
        EXPJOBQ       QUSRSYS             0     QBATCH          RLS
```

La gestión de líneas y dispositivos esta implícita en el perfil de usuario.

Dada la importancia de las acciones que este grupo puede realizar, se auditarán todos sus usuarios.

El perfil EXPLO no dispondrán de *SECADM, si bien podrán acceder los jefes de turno a la aplicación de usuarios para hacer uso de esta en "emergencias". Para ello se tendrá que modificar para permitir acceso restringido, pero plena funcionalidad.

Se mantiene el acceso habitual a la aplicación de usuarios.

Menú inicial (TSUTL/EXPLOTP): "`1. Aplicación de Usuarios`"

Que llama al programa TSAPUSU/GSTUSR.

Este perfil de usuario se eliminará del directorio del sistema y se modificará para que tenga un programa inicial a llamar que le asigne las librerías de trabajo.

Se crea el CL que asigna las bibliotecas de trabajo (TSUTL/CLINIEXP).

```
   Programa inicial a llamar  . . .   CLINIEXP
     Biblioteca . . . . . .     TSUTL
```

Lista de bibliotecas:

```
   QSYS        SYS
   QSYS2       SYS
   QHLPSYS     SYS
```

```
QUSRSYS      SYS
EXPLOT       CUR
CMDEXPLOT    USR
EXPLOT       USR
QGPL         USR
QTEMP        USR
```

No deben tener permisos para crear bibliotecas, modificar asignaciones de memoria o realizar modificaciones importantes en el sistema.

Gestión del Software de terceros

La gestión de herramientas, como EDITRAN, se realizará de la forma actual, si bien se generan nuevas puertas de acceso que mejoren la seguridad y proporcionen comodidad.

Se mantiene el modo habitual de trabajo:

Menú inicial (TSUTL/EXPLOTP): "`2. Menú de Transmisiones`"

Que llama al programa CFTUSER/MENUTRANS.

Se permite visualizar objetos en CFTUSER.

Menú inicial (TSUTL/EXPLOTP): "`8. Ver BCKPEN, BCKSEG y CFTUSER`"

Comando CMDEXPLOT/DSPSEGOBJ que llama al programa TSUTL/TSCLBU044.

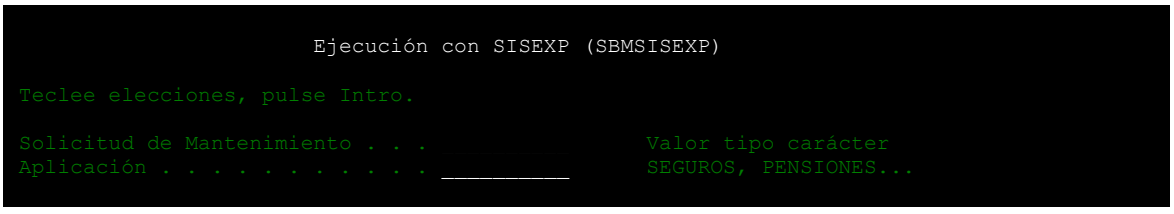
Otras

Se creará procedimiento para que, previa petición, puedan lanzar procesos con el usuario SISEXP.

Menú inicial (TSTUTL/EXPLOTP): "`9. Lanzar trabajo con SISEXP`"

Comando CMDEXPLOT/SBMSISEXP que llama al programa TSUTL/TSCLBU055.

Pantalla inicial:



Pantalla para SEGUROS/PENSIONES:

```
Solicitud de Mantenimiento . . . > CP00000       Valor tipo carácter
Aplicación . . . . . . . . . . . > SEGUROS       SEGUROS, PENSIONES, AMBOS...
Biblioteca del programa  . . . .   __________    Valor tipo carácter
Programa . . . . . . . . . . . .   __________    Valor tipo carácter
Generar log  . . . . . . . . . .   N             S, N
Parm. separados por espacios . .   ____________________________________________
```

Pantalla para OTROS:

```
Solicitud de Mantenimiento . . . > CP00000       Valor tipo carácter
Aplicación . . . . . . . . . . . > OTROS         SEGUROS, PENSIONES, AMBOS...
Descripcion de trabajo propia  .   *USRPRF       Valor tipo carácter
Biblioteca del programa  . . . .                 Valor tipo carácter
Programa . . . . . . . . . . . .                 Valor tipo carácter
Cola de trabajo  . . . . . . . .   *JOBD         Valor tipo carácter
Generar log  . . . . . . . . . .   N             S, N
Parm. separados por espacios . .   ____________________________________________
```

Librerías de datos de producción

AVF, PPDAT

Biblioteca: *USE

Objeto: Opr

El acceso a las librerías de datos estará restringido a la existencia del objeto pero no a su edición, modificación o visualización. También podrán visualizar los "atributos" de los ficheros.

No se permitirá ninguna acción adicional como creación, borrado, renombrar, mover, duplicar o cambiar autorizaciones dentro de las bibliotecas de programas.

No deben poder compilar programas.

Se permite modificar seldas.

Menú inicial (TSUTL/EXPLOTP): "3. Modificar SELDAS"

Comando CMDEXPLOT/CHGDTAEXP que llama al programa TSUTL/TSCLBU039.

Permite modificar AVF/SELDA1, AVF/DTACONTROL, PPDAT/PPDTA0, PPDAT/PPDTA1y PPDAT/DTACONTROL.

Se permite consultar y modificar FTPAGE y SEFTPAGE, buscando por condición o por parámetro.

Menú inicial (TSUTL/EXPLOTP): "6. Consultar FTPAGE/SEFTPAGE" y "7. Modificar FTPAGE/SEFTPAGE"

Comando DSPFTPAGE y UPDFTPAGE que llaman a los programas TSUTL/TSCLBU043 y TSUTL/TSCLBU045, respectivamente.

Librerías de programas: Fuentes y Objetos

EPTOOLS, PACOUTL, PPOBJ, PPSRC, OPNSPEN, SEC2077, OPNSSEG

Biblioteca: *USE

Objeto: Opr (excepto PACOUTL - *USE)

El acceso a las librerías de programas estará restringido a la comprobación de existencia del objeto pero no a su edición, modificación o visualización.

No se permitirá ninguna acción adicional como creación, borrado, renombrar, mover, duplicar o cambiar autorizaciones dentro de las bibliotecas de programas.

Se permite editar áreas de datos.

Se permite modificar seldas.

Menú inicial (TSUTL/EXPLOTP): "3. Modificar SELDAS"

Comando CHGDTAEXP que llama al programa TSUTL/TSCLBU039.

Permite modificar PACOUTL/SELDA0 y PACOUTL/SELDAIMP.

No deben poder compilar programas.

Librerías de seguridad: Bckseg/Bckpen/Spoolimp/Spoolsav

BCKSEG, BCKPEN, SPOOLSAV

Biblioteca: *EXCLUDE

Objeto: *EXCLUDE

No se permitirá ninguna acción dentro de esas bibliotecas debido al carácter de los datos que existen en ellas.

Se permite visualizar objetos en BCKSEG y BCKPEN.

Menú inicial (TSUTL/EXPLOTP): "`8. Ver BCKPEN, BCKSEG y CFTUSER`"

Comando `DSPSEGOBJ` que llama al programa TSUTL/TSCLBU044.

4.2.2. Departamento de Mantenimiento: Usuarios de Mantenimiento

El usuario del departamento de Mantenimiento que realice tareas de Mantenimiento pertenecerá al grupo MANTEN.

Este grupo será de perfil general *PGMR, añadiéndose el permiso *JOBCTL para poder seguir los trabajos que se ejecutan.

Los parámetros del pefil del grupo MANTEN serán:

```
Perfil de usuario  . . . . . > MANTEN        Nombre
Contraseña de usuario  . . . .   *NONE       Valor tipo carácter, *SAME...
Contraseña caducada  . . . . .   *NO         *SAME, *NO, *YES
Estado . . . . . .   *DISABLED   *SAME, *ENABLED, *DISABLED
Clase de usuario . . . . . .   *PGMR         *SAME, *USER, *SYSOPR...
Nivel de ayuda . . . . . .   *SYSVAL         *SAME, *SYSVAL, *BASIC...
Biblioteca actual  . . . . . .   MANLIB       Nombre, *SAME, *CRTDFT
Programa inicial a llamar  . . .   CLINIMAN   Nombre, *SAME, *NONE
  Biblioteca . . . . . .     TSUTL           Nombre, *LIBL, *CURLIB
Menú inicial . . . . . .   MANTEN            Nombre, *SAME, *SIGNOFF
  Biblioteca . . . . . .     TSUTL           Nombre, *LIBL, *CURLIB
Limitar posibilidades  . . . . .   *NO        *SAME, *NO, *PARTIAL, *YES
Texto descriptivo  . . . . . .   'Grupo de Mantenimiento'
                         Parámetros adicionales

Autorización especial  . . . . .   *JOBCTL    *SAME, *USRCLS, *NONE...
             + para más valores    *SPLCTL
Entorno especial . . . . . .   *SYSVAL       *SAME, *SYSVAL, *NONE, *S36
Visual informac inicio sesión  .   *SYSVAL   *SAME, *NO, *YES, *SYSVAL
Intervalo caducidad contraseña     *SYSVAL   1-366, *SAME, *SYSVAL, *NOMAX
Gestión de la contraseña local     *YES      *SAME, *YES, *NO
Limitar sesiones dispositivo . .   *YES      *SAME, *NO, *YES, *SYSVAL
Almacenam. intermedio teclado  .   *SYSVAL   *SAME, *SYSVAL, *NO...
Máx almacenamiento permitido . .   *NOMAX    Kilobytes, *SAME, *NOMAX
Máx prioridad planificación  . .   3         0-9, *SAME
Descripción de trabajo . . . . .   MANJOBD   Nombre, *SAME
  Biblioteca . . . . . .     QUSRSYS         Nombre, *LIBL, *CURLIB
Perfil de grupo  . . . . . .   *NONE         Nombre, *SAME, *NONE
Propietario  . . . . . .   *USRPRF           *SAME, *USRPRF, *GRPPRF
Autorización de grupo  . . . . .   *NONE      *SAME, *NONE, *ALL...
Tipo autorización grupo  . . . .   *PRIVATE   *PRIVATE, *PGP, *SAME
Grupos suplementarios  . . . . .   *NONE      Nombre, *SAME, *NONE
             + para más valores
Código de contabilidad . . . . .   *BLANK
Contraseña de documento  . . . .   *SAME      Nombre, *SAME, *NONE
Cola de mensajes . . . . . .   PRMAN          Nombre, *SAME, *USRPRF
  Biblioteca . . . . . .     QUSRSYS         Nombre, *LIBL, *CURLIB
Entrega  . . . . . .   *NOTIFY             *SAME, *NOTIFY, *BREAK...
Filtro del código de gravedad  .   0         0-99, *SAME
Dispositivo de impresión . . . .   *WRKSTN   Nombre, *SAME, *WRKSTN...
```

```
Cola de salida . . . . . .   *WRKSTN       Nombre, *SAME, *WRKSTN, *DEV
  Biblioteca . . . . . .                   Nombre, *LIBL, *CURLIB
Programa de atención . . . . .   *SYSVAL     Nombre, *SAME, *SYSVAL...
  Biblioteca . . . . . .                   Nombre, *LIBL, *CURLIB
Secuencia de ordenación  . . . .   *SYSVAL   Nombre, *SAME, *SYSVAL...
  Biblioteca . . . . . .                   Nombre, *LIBL, *CURLIB
ID de idioma . . . . . .   *SYSVAL       *SAME, *SYSVAL...
ID de país o región  . . . . .   *SYSVAL   *SAME, *SYSVAL...
ID de juego de caracteres  . . .   *SYSVAL *SAME, *SYSVAL, *HEX...
Control identif. caracteres  . .   *SYSVAL *SAME, *SYSVAL, *DEVD...
Atributos trab ent nacional  . .   *SYSVAL *SAME, *SYSVAL, *NONE...
             + para más valores
Entorno nacional . . . . . .   *SAME

Opciones de usuario  . . . . .   *NONE      *SAME, *NONE, *CLKWD...
             + para más valores
Número ID de usuario . . . . .   1147       1-4294967294, *SAME
Número ID de grupo . . . . . .   132        1-4294967294, *SAME, *GEN...
Directorio inicial . . . . . .   *SAME
Asociación EIM:
  Identificador EIM  . . . . .   *NOCHG
  Tipo de asociación . . . . .               *TARGET, *SOURCE, *TGTSRC...
  Acción de asociación . . . .               *REPLACE, *ADD, *REMOVE
  Crear identificador EIM  . . .             *NOCRTEIMID, *CRTEIMID
```

Y los perfiles de los usuarios vendrán definidos como:

```
Perfil usuario . . . . . :   MANxxx

Inicio sesión anterior . . . . . :   15/06/06  13:12:03
Intentos inicio sesión no válidos  . . . . :   0
Estado . . . . . :   *ENABLED
Fecha último cambio contraseña . . . . . :   04/05/06
Intervalo caducidad contraseña . . . . . :   *SYSVAL
  Fecha caducidad contraseña . . . . . :     03/07/06
Establecer contraseña en caducada  . . . . :   *NO
Gestión de la contraseña local . . . . . :   *YES
Clase usuario  . . . . . :   *PGMR
Autorizaciones especiales  . . . . . :   *NONE
Perfil grupo . . . . . :   MANTEN
Propietario  . . . . . :   *GRPPRF
Autorización grupo . . . . . :   *NONE
Tipo de autorización de grupo  . . . . . :   *PRIVATE
Grupos adicionales . . . . . :   *NONE
Nivel de ayuda . . . . . :   *SYSVAL
Biblioteca actual  . . . . . :   MANLIB
Programa inicial . . . . . :   CLINIMAN
  Biblioteca . . . . . :     TSUTL
Menú inicial . . . . . :   MANTEN
  Biblioteca . . . . . :     TSUTL
```

```
Limitar posibilidades  . . . . . :   *NO
Texto  . . . . . :   Perfil de xxx
Visualizar información inicio sesión . . . :   *SYSVAL
Limitar sesiones dispositivo . . . . . :   *YES
Almacenamiento intermedio teclado  . . . . :   *SYSVAL
Información de almacenamiento:
  Máximo almacenamiento permitido  . . . . :   *NOMAX
  Almacenamiento utilizado . . . . . :   3988
  Almacenamiento utilizado en ASP
    independiente  . . . . . :   *NO
Máxima prioridad planificación . . . . . :   3
Descripción trabajo  . . . . . :   MANJOBD
  Biblioteca . . . . . :     QUSRSYS
Código contabilidad  . . . . . :
Cola mensajes  . . . . . :   MANxxx
  Biblioteca . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . :   *NOTIFY
Gravedad cola mensajes . . . . . :   00
Cola salida  . . . . . :   *WRKSTN
  Biblioteca . . . . . :
Dispositivo impresora  . . . . . :   *WRKSTN
Entorno especial . . . . . :   *SYSVAL
Programa de atención . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Secuencia de ordenación  . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Identificador de idioma  . . . . . :   *SYSVAL
Identificador de país o región . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Opciones usuario . . . . . :   *NONE
Valor de auditoría de objeto . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
                                               *SYSMGT
Número de ID de usuario  . . . . . :   501
Número de ID de grupo  . . . . . :   *NONE
Directorio inicial . . . . . :   /home/MANxxx
```

No deben tener permisos para realizar salvados de datos, ya que en las máquinas de real no hay justificación para tal fin.

El permiso *SPLCTL debe ser otorgado pues sus incidencias se basan en gran medida en los resultados obtenidos por los procesos, resultados que van a “spool” de diversas colas, aunque no deben ser incluidos en el directorio del sistema.

Gestión del Sistema

No deben realizar ninguna gestión del sistema y habrá que limitar el acceso a ciertas acciones que se permiten por tener el perfil *PGMR, como comandos CHGJRN o CHGLICINF.

El lanzamiento de trabajos Batch y la ejecución de programas estarán permitidos, pero deberá asignársele una descripción de trabajo propia, limitándose el lanzamiento a QBATCH.

Para controlar estos lanzamientos se crea la descripción de trabajo MANJOBD que define que los trabajos saldrán por la cola de trabajos MANJOBQ que los ejecuta en el subsistema QBATCH.

Los parámetros con los que se define la descripción de trabajo MANJOBD son:

```
Descripción trabajo:   MANJOBD        Biblioteca:   QUSRSYS

Perfil usuario . . . . . . . . . . . . . . . . . :   *RQD
Comprobación sintaxis CL . . . . . . . . . . . . :   *NOCHK
Retener en cola de trabajos  . . . . . . . . . . :   *NO
Gravedad finalización  . . . . . . . . . . . . . :   30
Fecha trabajo  . . . . . . . . . . . . . . . . . :   *SYSVAL
Conmutadores trabajo . . . . . . . . . . . . . . :   00000000
Respuesta mensaje consulta . . . . . . . . . . . :   *RQD
Prioridad trabajo (en cola trabajos) . . . . . . :   5
Cola de trabajos . . . . . . . . . . . . . . . . :   MANJOBQ
  Biblioteca . . . . . . . . . . . . . . . . . . :     QUSRSYS
Prioridad salida (en cola salida)  . . . . . . . :   5
Dispositivo impresora  . . . . . . . . . . . . . :   *USRPRF
Cola salida  . . . . . . . . . . . . . . . . . . :   *USRPRF
  Biblioteca . . . . . . . . . . . . . . . . . . :
Anotación mensajes:
  Nivel  . . . . . . . . . . . . . . . . . . . . :   4
  Gravedad . . . . . . . . . . . . . . . . . . . :   0
```

```
  Texto  . . . . . . . . . . . . . . . . . . . . :   *NOLIST
Anotar mandatos programa CL  . . . . . . . . . . :   *NO
Código contabilidad  . . . . . . . . . . . . . . :   *USRPRF
Texto impresión  . . . . . . . . . . . . . . . . :   *SYSVAL
Datos direccionamiento . . . . . . . . . . . . . :   QCMDI
Datos petición . . . . . . . . . . . . . . . . . :   *NONE
Conversación de DDM  . . . . . . . . . . . . . . :   *KEEP
Acción recuperación dispositivo  . . . . . . . . :   *SYSVAL
Agrupación fin porción tiempo  . . . . . . . . . :   *SYSVAL
Tamaño máximo de cola de mensajes del trabajo  . :   *SYSVAL
Acción para cola de mensajes de trabajo llena  . :   *SYSVAL
Permitir múltiples hebras  . . . . . . . . . . . :   *NO
Grupo de ASP inicial . . . . . . . . . . . . . . :   *NONE
Acción de archivo en spool . . . . . . . . . . . :   *SYSVAL
Texto  . . . . . . . . . . . . . . . . . . . . . :   Descripción de trabajo grupo
Mantenimiento
```

Y la cola por la que se ejecutan los trabajos es:

```
Cola          Biblioteca     Trbjos     Subsistema     Estado
MANJOBQ       QUSRSYS             0     QBATCH          RLS
```

Se permite el uso de SDA, DFU, SQL y QUERY pero se limitan las sesiones en real a 1 por máquina/usuario.

Existe un parámetro en el perfil del usuario que permite definir esta limitación.

```
Limitar sesiones dispositivo . .   *YES
```

Debido a las acciones que realizan estos usuarios deben ser auditados.

Se auditarán todos los objetos que sean accedidos por los usuarios.

Se definen todas las acciones que deben ser auditadas en el perfil del usuario.

```
Valor de auditoría de objeto . . . . . :   *ALL
Valores de auditoría de acciones . . . . :   *CMD
                                             *CREATE
                                             *DELETE
                                             *JOBDTA
                                             *OBJMGT
                                             *PGMADP
                                             *SAVRST
                                             *SECURITY
                                             *SERVICE
```

```
                                        *SPLFDTA
                                        *SYSMGT
```

Para cargar correctamente la lista de bibliotecas, se crea un CL que lee de un fichero las bibliotecas a cargar y su orden (TSUTL/CLINIMAN). Este listado ha sido definido con el grupo de mantenimiento de acuerdo a sus necesidades de trabajo.

La lista de bibliotecas es:

```
QSYS         SYS
QSYS2        SYS
QHLPSYS      SYS
QUSRSYS      SYS
MANLIB       CUR
CMDMANTEN    USR
AVF          USR
PPDAT        USR
FTESSEG      USR
SEC2077      USR
FTESPEN      USR
PPOBJ        USR
PPSRC        USR
PACOUTL      USR
CFTUSER      USR
AVP          USR
QGPL         USR
QTEMP        USR
```

Gestión del Software de terceros

No podrán modificar, borrar, crear, o realizar acción alguna sobre el software de terceros (EDITRAN,…) ni tampoco hacer uso de él para realizar envíos, etc....

Librerías de datos de producción

AVF, PPDAT, AVP Biblioteca: *CHANGE Objeto: *CHANGE + Gest (para CLRPFM)

El acceso a las librerías de datos estará restringido a la existencia y edición de ficheros. No se permitirá ninguna acción adicional como crear, borrar, renombrar, mover, duplicar o cambiar autorizaciones dentro de las bibliotecas de producción.

Se permitirá la copia de objetos a una biblioteca de trabajo (CPYOBJMAN).

Se permite copiar objetos de AVF/PPDAT a MANLIB.

Menú inicial (TSUTL/MANTEN): "6. Copiar de AVF/PPDAT/BCKPEN/BCKSEG/CFTUSER"

Comando CPYOBJMAN que llama al programa TSUTL/TSCLBU046.

Se permite modificar seldas de AVF/PPDAT.

Menú inicial (TSUTL/MANTEN): "7. Modificar Selda en AVF/PPDAT/PACOUTL "

Comando CHGDTAMAN que llama al programa TSUTL/TSCLBU062.

Librería de programas: Fuentes y Objetos

EPTOOLS, PACOUTL, PPOBJ, PPSRC, OPNSPEN, SEC2077, OPNSSEG Biblioteca: *USE (excepto EPTOOLS → *CHANGE) Objeto: *USE (excepto EPTOOLS→ *ALL; PACOUTL → *CHANGE)

El acceso a las librerías de programas estará restringido a la comprobación de existencia del objeto pero no a su edición, modificación.

No se permitirá ninguna acción adicional como creación, borrado, renombrar, mover, duplicar o cambiar autorizaciones dentro de las bibliotecas de programas.

Se permite compilar programas sobre la biblioteca MANLIB.

Se permite modificar seldas de PACOUTL.

Menú inicial (TSUTL/MANTEN): "7. Modificar Selda en AVF/PPDAT/PACOUTL "

Comando CHGDTAMAN que llama al programa TSUTL/TSCLBU062.

Libería de seguridad: Bckseg/Bckpen/Spoolimp/Spoolsav

BCKSEG, BCKPEN, SPOOLSAV Biblioteca: *CHANGE (excepto SPOOLSAV --> *USE) Objeto: *USE

Se permitirá la comprobación de existencia y la visualización de los datos de los objetos contenidos en la biblioteca. Ninguna acción adicional será permitida.

Se permite copiar los objetos de Bckseg/Bckpen/Spoolsav.

Se permite renombrar objetos en BCKPEN/BCKSEG/IMPRPRIMP.

Menú inicial (TSUTL/MANTEN): "2. Renombrar objeto en BCKPEN/BCKSEG/CFTUSER/IMPRPRIMP"

Comando RNMOBJBCK que llama al programa TSUTL/TSCLBU049.

Se permite copiar objetos de BCKPEN/BCKSEG a MANLIB.

Menú inicial (TSUTL/MANTEN): "6. Copiar de AVF/PPDAT/BCKPEN/BCKSEG/CFTUSER"

Comando CPYOBJMAN que llama al programa TSUTL/TSCLBU046.

4.2.3. Departamento de Mantenimiento: Usuarios de GET

El usuario del departamento que realice tareas de Mantenimiento pertenecerá al grupo GET.

Este grupo será de perfil general *PGMR, añadiéndose el permiso *JOBCTL para poder seguir los trabajos que se ejecutan.

El perfil del grupo GET quedará como sigue:

```
Perfil usuario . . . . . :   GET
Inicio sesión anterior . . . . . :
Intentos inicio sesión no válidos  . . . . :   0
Estado . . . . . :   *DISABLED
Fecha último cambio contraseña . . . . . :   11/06/06
Intervalo caducidad contraseña . . . . . :   *SYSVAL
  Fecha caducidad contraseña . . . . . :     10/08/06
Establecer contraseña en caducada  . . . . :   *NO
Gestión de la contraseña local . . . . . :   *YES
Clase usuario  . . . . . :   *PGMR
Autorizaciones especiales  . . . . . :   *NONE
Perfil grupo . . . . . :   *NONE
Propietario  . . . . . :   *USRPRF
Autorización grupo . . . . . :   *NONE
Tipo de autorización de grupo  . . . . . :   *PRIVATE
Grupos adicionales . . . . . :   *NONE
Nivel de ayuda . . . . . :   *SYSVAL
Biblioteca actual  . . . . . :   MANLIB
Programa inicial . . . . . :   CLINIGET
  Biblioteca . . . . . :     TSUTL
Menú inicial . . . . . :   GETMNU
  Biblioteca . . . . . :     TSUTL
Limitar posibilidades  . . . . . :   *NO
Texto  . . . . . :   Grupo de Get
Visualizar información inicio sesión . . . :   *SYSVAL
Limitar sesiones dispositivo . . . . . :   *YES
Almacenamiento intermedio teclado  . . . . :   *SYSVAL
Información de almacenamiento:
  Máximo almacenamiento permitido  . . . . :   *NOMAX
  Almacenamiento utilizado . . . . . :   12
  Almacenamiento utilizado en ASP
    independiente  . . . . . :   *NO
Máxima prioridad planificación . . . . . :   3
Descripción trabajo  . . . . . :   GETJOBD
  Biblioteca . . . . . :     QUSRSYS
Código contabilidad  . . . . . :
Cola mensajes  . . . . . :   GET
  Biblioteca . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . :   *NOTIFY
Gravedad cola mensajes . . . . . :   00
```

```
Cola salida  . . . . . :   *WRKSTN
  Biblioteca . . . . . :
Dispositivo impresora  . . . . . :   *WRKSTN
Entorno especial . . . . . :   *SYSVAL
Programa de atención . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Secuencia de ordenación  . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Identificador de idioma  . . . . . :   *SYSVAL
Identificador de país o región . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Opciones usuario . . . . . :   *NONE
Valor de auditoría de objeto . . . . . :   *NONE
Valores de auditoría de acciones . . . . . :   *NONE
Número de ID de usuario  . . . . . :   1223
Número de ID de grupo  . . . . . :   136
Directorio inicial . . . . . :   /home/GET
```

Se definirá el perfil de los usuarios GET con los siguientes parámetros:

```
Perfil usuario . . . . . :   GETxxx
Inicio sesión anterior . . . . . :   05/04/05  23:58:48
Intentos inicio sesión no válidos  . . . . :   0
Estado . . . . . :   *ENABLED
Fecha último cambio contraseña . . . . . :   05/04/05
Intervalo caducidad contraseña . . . . . :   *SYSVAL
  Fecha caducidad contraseña . . . . . :     04/06/05
Establecer contraseña en caducada  . . . . :   *NO
Gestión de la contraseña local . . . . . :   *YES
Clase usuario  . . . . . :   *PGMR
Autorizaciones especiales  . . . . . :   *NONE
Perfil grupo . . . . . :   MANTEN
Propietario  . . . . . :   *GRPPRF
Autorización grupo . . . . . :   *NONE
Tipo de autorización de grupo  . . . . . :   *PRIVATE
Grupos adicionales . . . . . :   GET
Nivel de ayuda . . . . . :   *SYSVAL
Biblioteca actual  . . . . . :   MANLIB
Programa inicial . . . . . :   CLINIGET
  Biblioteca . . . . . :     TSUTL
Menú inicial . . . . . :   GETMNU
  Biblioteca . . . . . :     TSUTL
Limitar posibilidades  . . . . . :   *NO
Texto  . . . . . :   Perfil de GET
Visualizar información inicio sesión . . . :   *SYSVAL
Limitar sesiones dispositivo . . . . . :   *SYSVAL
Almacenamiento intermedio teclado  . . . . :   *SYSVAL
```

```
Información de almacenamiento:
  Máximo almacenamiento permitido  . . . . :   *NOMAX
  Almacenamiento utilizado . . . . . . . . :   12
  Almacenamiento utilizado en ASP
    independiente  . . . . . . . . . . . . :   *NO
Máxima prioridad planificación . . . . . . :   3
Descripción trabajo  . . . . . . . . . . . :   GETJOBD
  Biblioteca . . . . . . . . . . . . . . . :     QUSRSYS
Código contabilidad  . . . . . . . . . . . :
Cola mensajes  . . . . . . . . . . . . . . :   GETxxx
  Biblioteca . . . . . . . . . . . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . . . . . . :   *NOTIFY
Gravedad cola mensajes . . . . . . . . . . :   00
Cola salida  . . . . . . . . . . . . . . . :   *WRKSTN
  Biblioteca . . . . . . . . . . . . . . . :
Dispositivo impresora  . . . . . . . . . . :   *WRKSTN
Entorno especial . . . . . . . . . . . . . :   *SYSVAL
Programa de atención . . . . . . . . . . . :   *SYSVAL
  Biblioteca . . . . . . . . . . . . . . . :
Secuencia de ordenación  . . . . . . . . . :   *SYSVAL
  Biblioteca . . . . . . . . . . . . . . . :
Identificador de idioma  . . . . . . . . . :   *SYSVAL
Identificador de país o región . . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . . . . . . . . . :   *SYSVAL
Opciones usuario . . . . . . . . . . . . . :   *NONE
Valor de auditoría de objeto . . . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
                                               *SYSMGT
Número de ID de usuario  . . . . . . . . . :   786
Número de ID de grupo  . . . . . . . . . . :   *NONE
Directorio inicial . . . . . . . . . . . . :   /home/GETxxx
```

No deben tener permisos para realizar salvados de datos, ya que en las máquinas de real no hay justificación para tal fin.

El permiso de SPLCTL debe ser otorgado pues sus incidencias se basan en gran medida en los resultados obtenidos por los procesos, resultados que van a Spools de diversas colas, aunque no deben ser incluidos en el directorio del sistema.

```
Permiso *SPLCTL.
 Autorización especial  . . . . .   *JOBCTL
              + para más valores    *SPLCTL
```

Se dispondrá de una biblioteca para poder copiar datos para trabajar sobre ellos. Se define MANTEN como biblioteca de trabajo que será utilizada para que se creen los objetos temporales que se requieran.

Dado el alto nivel de autorización que requiere este grupo y su limitación al horario nocturno, se debe evitar que estos usuarios se puedan utilizar durante la jornada diurna, por lo que este grupo se habilitará en horario de 19:00 a 9:30, mientras que, en otro horario estará en modo DISABLED.

Para activar, y desactivar, este grupo, se añadirán al planificador del AS400 dos trabajos que activarán y desactivarán los usuarios a las horas indicadas.

```
                    ---Planificación---  Frecuen-
Trabajo     Estado  Fecha      Hora      cia
ACTIVAGET    SCD    DEF USUAR  19:00:00  *WEEKLY
DESACTIGET   SCD    DEF USUAR  09:30:00  *WEEKLY
```

Como el planificador del AS400 no contempla un tratamiento para los días festivos, en caso de necesitar habilitar un usuario en festivo (o cualquier otra situación fuera de horas habilitadas) se deberá solicitar el desbloqueo a Explotación.

Gestión del Sistema

No deben realizar ninguna gestión del sistema y habrá que limitar el acceso a ciertas acciones que se permiten por tener el perfil QPGMR como comando CHJRN o CHGLICINF.

El lanzamiento de trabajos “batch” y la ejecución de programas estará permitida, pero deberá asignársele una descripción de trabajo propia, limitándose el lanzamiento al subsistema QBATCH.

Para ello se crea la descripción de trabajo GETJOBD que define que se podrá ejecutar simultáneamente 1 trabajo como máximo y que los trabajos saldrán por la cola de trabajos GETJOBQ, que, a su vez, ejecutará los trabajos en el subsistema QBATCH.

La descripción de trabajo GETJOBD quedará definida de la siguiente manera:

```
Descripción trabajo:   GETJOBD        Biblioteca:   QUSRSYS
Perfil usuario . . . . . . . . . . . . . . . . . :   *RQD
Comprobación sintaxis CL . . . . . . . . . . . . :   *NOCHK
Retener en cola de trabajos  . . . . . . . . . . :   *NO
Gravedad finalización  . . . . . . . . . . . . . :   30
Fecha trabajo  . . . . . . . . . . . . . . . . . :   *SYSVAL
Conmutadores trabajo . . . . . . . . . . . . . . :   00000000
Respuesta mensaje consulta . . . . . . . . . . . :   *RQD
Prioridad trabajo (en cola trabajos) . . . . . . :   5
Cola de trabajos . . . . . . . . . . . . . . . . :   MANJOBQ
  Biblioteca . . . . . . . . . . . . . . . . . . :     QUSRSYS
Prioridad salida (en cola salida)  . . . . . . . :   5
Dispositivo impresora  . . . . . . . . . . . . . :   *USRPRF
Cola salida  . . . . . . . . . . . . . . . . . . :   *USRPRF
  Biblioteca . . . . . . . . . . . . . . . . . . :
Anotación mensajes:
  Nivel  . . . . . . . . . . . . . . . . . . . . :   4
  Gravedad . . . . . . . . . . . . . . . . . . . :   0
  Texto  . . . . . . . . . . . . . . . . . . . . :   *NOLIST
Anotar mandatos programa CL  . . . . . . . . . . :   *NO
Código contabilidad  . . . . . . . . . . . . . . :   *USRPRF
Texto impresión  . . . . . . . . . . . . . . . . :   *SYSVAL
Datos direccionamiento . . . . . . . . . . . . . :   QCMDI
Datos petición . . . . . . . . . . . . . . . . . :   *NONE
Conversación de DDM  . . . . . . . . . . . . . . :   *KEEP
Acción recuperación dispositivo  . . . . . . . . :   *SYSVAL
Agrupación fin porción tiempo  . . . . . . . . . :   *SYSVAL
Tamaño máximo de cola de mensajes del trabajo  . :   *SYSVAL
Acción para cola de mensajes de trabajo llena  . :   *SYSVAL
Permitir múltiples hebras  . . . . . . . . . . . :   *NO
Grupo de ASP inicial . . . . . . . . . . . . . . :   *NONE
Acción de archivo en spool . . . . . . . . . . . :   *SYSVAL
Texto  . . . . . . . . . . . . . . . . . . . . . :   Descripción de trabajo Grupo
GET
```

Y la cola de salida de los trabajos se definirá como:

```
Cola           Biblioteca     Trbjos     Subsistema     Estado
GETJOBQ        QUSRSYS             0     QBATCH          RLS
```

Se permitirá el uso de herramientas de programación como el SDA, DFU, SQL y QUERY, pero se limitarán el número de sesiones por máquina y usuario a 1.

Se definirá el perfil de usuario como:

```
    Limitar sesiones dispositivo . .   *YES
```

Debido a las acciones que realizan estos usuarios deben ser auditados.

Se auditarán todas las acciones realizadas sobre todos los objetos.

```
Valor de auditoría de objeto . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
                                               *SYSMGT
```

Librerías de datos de producción

AVF, PPDAT, AVP Biblioteca: *CHANGE Objetos: *CHANGE + Gest + Exist

El acceso a las librerías de datos estará restringido a existencia y edición de ficheros, se permitirá la copia de objetos a una biblioteca de trabajo.

Debido al modo de trabajo del personal del GET se permitirá el borrado de ficheros y el renombrado de estos.

Cualquier acción realizada debe ser notificada al grupo de Sistemas.

Pueden crear objetos en producción.

Librería de programas: Fuentes y Objetos

EPTOOLS, PACOUTL, PPOBJ, PPSRC, OPNSPEN, SEC2077, OPNSSEG

Biblioteca: *CHANGE

Objeto: *ALL

Debido a las actuaciones de emergencia se permite el control total sobre las librerías de programas.

Librería de seguridad: Bckseg/Bckpen/Spoolimp/Spoolsav

BCKSEG, BCKPEN, SPOOLSAV

Biblioteca: *CHANGE (excepto SPOOLSAV --> *ALL)

Objeto: *ALL

Se permite la visualización, movimiento y renombrado de los objetos.

Gestión del software de terceros

No podrán visualizar, modificar, borrar, crear o realizar acción alguna sobre el software de terceros (EDITRAN,...) ni tampoco hacer uso de él para envíos, etc...

Se les permite las mismas modificaciones que los usuarios del grupo MANTEN.

Se permite renombrar objetos en CFTUSER.

Menú inicial (TSUTL/MANTEN): "2. Renombrar objeto en BCKPEN/BCKSEG/CFTUSER/IMPRPRIMP"

Comando RNMOBJBCK que llama al programa TSUTL/TSCLBU049.

Se permite copiar objetos de CFTUSER a MANLIB.

Menú inicial (TSUTL/MANTEN): "6. Copiar de AVF/PPDAT/BCKPEN/BCKSEG/CFTUSER"

Comando CPYOBJMAN que llama al programa TSUTL/TSCLBU046.

4.2.4. Usuario especial Sisexp: Planificador

Este usuario corresponde con el utilizado por el planificador (PACO) utilizado para la explotación nocturna, bajo este usuario se ejecutan los procesos “batch”.

El usuario SISEXP deberá pertenecer al perfil de *SYSOPR debido a que necesita *JOBCTL y *SAVSYS para realizar sus tareas.

```
Perfil usuario . . . . . :   SISEXP
Inicio sesión anterior . . . . . :   19/06/06  09:48:44
Intentos inicio sesión no válidos  . . . . :   0
Estado . . . . . :   *ENABLED
Fecha último cambio contraseña . . . . . :   28/05/06
Intervalo caducidad contraseña . . . . . :   *SYSVAL
  Fecha caducidad contraseña . . . . . :     27/07/06
Establecer contraseña en caducada  . . . . :   *NO
Gestión de la contraseña local . . . . . :   *YES
Clase usuario  . . . . . :   *SYSOPR
Autorizaciones especiales  . . . . . :   *JOBCTL
                                         *SAVSYS
                                         *SPLCTL
Perfil grupo . . . . . :   *NONE
Propietario  . . . . . :   *USRPRF
Autorización grupo . . . . . :   *NONE
Tipo de autorización de grupo  . . . . . :   *PRIVATE
Grupos adicionales . . . . . :   *NONE
Nivel de ayuda . . . . . :   *SYSVAL
Biblioteca actual  . . . . . :   *CRTDFT
Programa inicial . . . . . :   *NONE
  Biblioteca . . . . . :
Menú inicial . . . . . :   MAIN
  Biblioteca . . . . . :     QSYS
Limitar posibilidades  . . . . . :   *NO
Texto  . . . . . :   * * * AUTO PLANIFICADOR * * *
Visualizar información inicio sesión . . . :   *SYSVAL
Limitar sesiones dispositivo . . . . . :   *YES
Almacenamiento intermedio teclado  . . . . :   *SYSVAL
Información de almacenamiento:
  Máximo almacenamiento permitido  . . . . :   *NOMAX
  Almacenamiento utilizado . . . . . :   59171772
  Almacenamiento utilizado en ASP
    independiente  . . . . . :   *NO
Máxima prioridad planificación . . . . . :   3
Descripción trabajo  . . . . . :   QDFTJOBD
  Biblioteca . . . . . :     QGPL
Código contabilidad  . . . . . :
Cola mensajes  . . . . . :   SISEXP
```

```
  Biblioteca . . . . . . . . . . . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . . . . . . :   *NOTIFY
Gravedad cola mensajes . . . . . . . . . . :   00
Cola salida  . . . . . . . . . . . . . . . :   QSISEXP
  Biblioteca . . . . . . . . . . . . . . . :     QUSRSYS
Dispositivo impresora  . . . . . . . . . . :   *WRKSTN
Entorno especial . . . . . . . . . . . . . :   *SYSVAL
Programa de atención . . . . . . . . . . . :   *SYSVAL
  Biblioteca . . . . . . . . . . . . . . . :
Secuencia de ordenación  . . . . . . . . . :   *SYSVAL
  Biblioteca . . . . . . . . . . . . . . . :
Identificador de idioma  . . . . . . . . . :   *SYSVAL
Identificador de país o región . . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . . . . . . . . . :   *SYSVAL
Opciones usuario . . . . . . . . . . . . . :   *NONE
Valor de auditoría de objeto . . . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
                                               *SYSMGT
Número de ID de usuario  . . . . . . . . . :   285
Número de ID de grupo  . . . . . . . . . . :   *NONE
Directorio inicial . . . . . . . . . . . . :   /home/SISEXP
```

Está limitado a una sesión interactiva por máquina.

```
   Limitar sesiones dispositivo . .   *YES
```

Gestión del sistema

El usuario SISEXP, aunque no tiene por qué modificar el sistema, realiza comandos como WRKSYSSTS, DSPMSG QSYSOPR, etc... por lo que el perfil *QSYSOPR es perfectamente válido.

Debido a la diferencia de permisos con Explotación, éste no puede ser del mismo grupo.

NO hace falta SECADM debido a que se ha utilizado SWITCH de usuarios para realizar la habilitación/inhabilitación de usuarios y el proceso se ejecuta con otro usuario.

Gestión del Software de terceros

Debe poder "usar" el software de terceros, al igual que el software de la aplicación.

Se requiere permisos sobre las descripciones de trabajo utilizadas por el planificador (PACOPEND, PACOPENDP, PACOSEGD, PACOSEGDP, PACOUSUPPD y PACOUSUSED).

Permisos sobre los colas de salida utilizadas en las anteriores descripciones (PENSIONES, PENSION, SEGUROS, DESARROLLO, PENSIONES y SEGUROS).

Permisos sobre las bibliotecas (y sus objetos) de la lista de las bibliotecas de las descripciones de trabajo PACO*.

Permisos sobre el dispositivo y la cola de salida utilizada por el usuario SISEXP.

Permisos sobre las bibliotecas anotadas en la selda PACOUTL/SELDA0.

Permisos en la biblioteca (y sus objetos) AUXPAQ, CRIPTDES y EDITRAN41.

Permisos sobre el usuario EDITRAN41.

Permisos sobre los comandos SAVOBJBRM, SAVOBJ, RSTOBJBRM, RSTOBJ, SAVLIB y SAV.

Permisos sobre QSYSOPR.

Permisos sobre la biblioteca (y sus objetos) CRIPTO y PKZ560510.

Permisos sobre bibliotecas (y objetos) del salvado diario correspondiente. Revisión de las llamadas *EXIT.

Permisos sobre la descripción de trabajo SCAID.

Librerías de datos de producción

AVF, PPDAT, AVP Biblioteca: *CHANGE Objeto: *ALL

Obviamente tiene que tener control TOTAL sobre los objetos contenidos, pero no debe poder borrar el objeto biblioteca.

Libería de programas: Fuentes y Objetos

EPTOOLS, PACOUTL, PPOBJ, PPSRC, OPNSPEN, SEC2077, OPNSSEG Biblioteca: *CHANGE Objeto: *ALL

Debido a la creación de objetos temporales en las diferentes bibliotecas y hasta que se proceda a la "depuración" de estos procesos se otorgan permisos *ALL.

Librería de seguridad: Bckseg/Bckpen/Spoolimp/Spoolsav

BCKSEG, BCKPEN, SPOOLSAV Biblioteca: *CHANGE Objeto: *ALL

Obviamente tiene que tener control TOTAL sobre los objetos contenidos pero no debe poder borrar el objeto biblioteca.

4.2.5. Usuarios de Sistemas

Los usuarios de Sistemas deberán tener perfil *SYSOPR si bien necesitan permisos adicionales como *SERVICE, *AUDIT, *SPLCTL....

Dado que estas acciones serán “puntuales” se deberán generar otros modos de acceso para realizar estas tareas donde se carezca de permisos.

El perfil del grupo de usuarios se define como:

```
        Perfil usuario . . . . . . . . . . . . . :   TSISTEMAS
        Inicio sesión anterior . . . . . . . . . :
        Intentos inicio sesión no válidos  . . . . :   0
        Estado . . . . . . . . . . . . . . . . . :   *DISABLED
        Fecha último cambio contraseña . . . . . :   20/04/04
        Intervalo caducidad contraseña . . . . . :   *SYSVAL
          Fecha caducidad contraseña . . . . . :     19/06/04
        Establecer contraseña en caducada  . . . . :   *NO
        Gestión de la contraseña local . . . . . :   *YES
        Clase usuario  . . . . . . . . . . . . . :   *SYSOPR
        Autorizaciones especiales  . . . . . . . :   *NONE
        Perfil grupo . . . . . . . . . . . . . . :   *NONE
        Propietario  . . . . . . . . . . . . . . :   *USRPRF
        Autorización grupo . . . . . . . . . . . :   *NONE
        Tipo de autorización de grupo  . . . . . :   *PRIVATE
        Grupos adicionales . . . . . . . . . . . :   *NONE
        Nivel de ayuda . . . . . . . . . . . . . :   *SYSVAL
        Biblioteca actual  . . . . . . . . . . . :   *CRTDFT
        Programa inicial . . . . . . . . . . . . :   *NONE
          Biblioteca . . . . . . . . . . . . . . :
        Menú inicial . . . . . . . . . . . . . . :   MAIN
          Biblioteca . . . . . . . . . . . . . . :     *LIBL
        Limitar posibilidades  . . . . . . . . . :   *NO
        Texto  . . . . . . . . . . . . . . . . . :   Perfil de grupo para Técnica de
sistemas
Visualizar información inicio sesión . . . :   *SYSVAL
        Limitar sesiones dispositivo . . . . . . :   *SYSVAL
        Almacenamiento intermedio teclado  . . . . :   *SYSVAL
        Información de almacenamiento:
          Máximo almacenamiento permitido  . . . . :   *NOMAX
          Almacenamiento utilizado . . . . . . . . :   10174996
          Almacenamiento utilizado en ASP
            independiente  . . . . . . . . . . . . :   *NO
        Máxima prioridad planificación . . . . . . :   3
        Descripción trabajo  . . . . . . . . . . . :   QDFTJOBD
          Biblioteca . . . . . . . . . . . . . . :     QGPL
        Código contabilidad  . . . . . . . . . . . :
```

```
Cola mensajes  . . . . . :   TSISTEMAS
  Biblioteca . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . :   *NOTIFY
Gravedad cola mensajes . . . . . :   00
Cola salida  . . . . . :   *WRKSTN
  Biblioteca . . . . . :
Dispositivo impresora  . . . . . :   *WRKSTN
Entorno especial . . . . . :   *SYSVAL
Programa de atención . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Secuencia de ordenación  . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Identificador de idioma  . . . . . :   *SYSVAL
Identificador de país o región . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Valor de auditoría de objeto . . . . . :   *NONE
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
                                               *SYSMGT
Número de ID de usuario  . . . . . :   651
Número de ID de grupo  . . . . . :   125
Directorio inicial . . . . . :   /home/TSISTEMAS
```

Y el perfil de los usuarios se definirá como:

```
Perfil usuario . . . . . :   TSIxxx
Inicio sesión anterior . . . . . :   19/06/06  12:56:23
Intentos inicio sesión no válidos  . . . . :   0
Estado . . . . . :   *ENABLED
Fecha último cambio contraseña . . . . . :   12/05/06
Intervalo caducidad contraseña . . . . . :   *SYSVAL
  Fecha caducidad contraseña . . . . . :     11/07/06
Establecer contraseña en caducada  . . . . :   *NO
Gestión de la contraseña local . . . . . :   *YES
Clase usuario  . . . . . :   *SYSOPR
Autorizaciones especiales  . . . . . :   *JOBCTL
                                         *SAVSYS
                                         *SPLCTL
```

```
Perfil grupo . . . . . :   TSISTEMAS
Propietario  . . . . . :   *GRPPRF
Autorización grupo . . . . . :   *NONE
Tipo de autorización de grupo  . . . . . :   *PRIVATE
Grupos adicionales . . . . . :   *NONE
Nivel de ayuda . . . . . :   *SYSVAL
Biblioteca actual  . . . . . :   *CRTDFT
Programa inicial . . . . . :   *NONE
  Biblioteca . . . . . :
Menú inicial . . . . . :   SISTEMAS
  Biblioteca . . . . . :     TSUTL
Limitar posibilidades  . . . . . :   *NO
Texto  . . . . . :   Perfil de xxx
Visualizar información inicio sesión . . . :   *SYSVAL
Limitar sesiones dispositivo . . . . . :   *SYSVAL
Almacenamiento intermedio teclado  . . . . :   *SYSVAL
Información de almacenamiento:
  Máximo almacenamiento permitido  . . . . :   *NOMAX
  Almacenamiento utilizado . . . . . :   31479528
  Almacenamiento utilizado en ASP
    independiente  . . . . . :   *NO
Máxima prioridad planificación . . . . . :   3
Descripción trabajo  . . . . . :   QDFTJOBD
  Biblioteca . . . . . :     QGPL
Código contabilidad  . . . . . :
Cola mensajes  . . . . . :   TSxxx
  Biblioteca . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . :   *BREAK
Gravedad cola mensajes . . . . . :   00
Cola salida  . . . . . :   *WRKSTN
  Biblioteca . . . . . :
Dispositivo impresora  . . . . . :   *WRKSTN
Entorno especial . . . . . :   *SYSVAL
Programa de atención . . . . . :   USUARIOS
  Biblioteca . . . . . :     TSAPUSU
Secuencia de ordenación  . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Identificador de idioma  . . . . . :   *SYSVAL
Identificador de país o región . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Opciones usuario . . . . . :   *NONE
Valor de auditoría de objeto . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
```

```
                                                *SAVRST
                                                *SECURITY
                                                *SERVICE
                                                *SPLFDTA
                                                *SYSMGT
Número de ID de usuario  . . . . . :   432
Número de ID de grupo  . . . . . :   *NONE
Directorio inicial . . . . . :   /home/TSxxx
```

Las autorizaciones se centrarán en la gestión del sistema y las bibliotecas de “software de terceros”, evitando el acceso a datos en la mayor medida posible.

Deben establecerse mecanismos de control para poder supervisar los cambios de los valores del sistema.

Se deberá crear un usuario para poder ejecutar los "comandos especiales" y con el que no se podrá iniciar sesión, solamente servirá para la ejecución de tareas específicas que requieran de más permisos de los que se ha definido el usuario “habitual”.

Se crean los usuario SUPxxx (con contraseña *NONE), para realizar aquellas tareas que necesitan permisos adicionales.

Su perfil quedará de este modo:

```
Perfil usuario . . . . . :   SUPxxx
Inicio sesión anterior . . . . . :
Intentos inicio sesión no válidos  . . . . :   0
Estado . . . . . :   *ENABLED
Fecha último cambio contraseña . . . . . :   05/06/06
Intervalo caducidad contraseña . . . . . :   *SYSVAL
  Fecha caducidad contraseña . . . . . :     04/08/06
Establecer contraseña en caducada  . . . . :   *NO
Gestión de la contraseña local . . . . . :   *YES
Clase usuario  . . . . . :   *SECOFR
Autorizaciones especiales  . . . . . :   *ALLOBJ
                                                *AUDIT
                                                *IOSYSCFG
                                                *JOBCTL
                                                *SAVSYS
                                                *SECADM
                                                *SPLCTL
Perfil grupo . . . . . :   TSISTEMAS
Propietario  . . . . . :   *GRPPRF
Autorización grupo . . . . . :   *NONE
Tipo de autorización de grupo  . . . . . :   *PRIVATE
```

```
Grupos adicionales . . . . . :   *NONE
Nivel de ayuda . . . . . :   *SYSVAL
Biblioteca actual  . . . . . :   *CRTDFT
Programa inicial . . . . . :   *NONE
  Biblioteca . . . . . :
Menú inicial . . . . . :   SISTEMAS
  Biblioteca . . . . . :     TSUTL
Limitar posibilidades  . . . . . :   *NO
Texto  . . . . . :   Perfil SUP de xxx
Visualizar información inicio sesión . . . :   *SYSVAL
Limitar sesiones dispositivo . . . . . :   *SYSVAL
Almacenamiento intermedio teclado  . . . . :   *SYSVAL
Información de almacenamiento:
  Máximo almacenamiento permitido  . . . . :   *NOMAX
  Almacenamiento utilizado . . . . . :   1840
  Almacenamiento utilizado en ASP
    independiente  . . . . . :   *NO
Máxima prioridad planificación . . . . . :   3
Descripción trabajo  . . . . . :   QDFTJOBD
  Biblioteca . . . . . :     QGPL
Código contabilidad  . . . . . :
Cola mensajes  . . . . . :   SUPxxx
  Biblioteca . . . . . :     QUSRSYS
Entrega cola mensajes  . . . . . :   *BREAK
Gravedad cola mensajes . . . . . :   00
Cola salida  . . . . . :   *WRKSTN
  Biblioteca . . . . . :
Dispositivo impresora  . . . . . :   *WRKSTN
Entorno especial . . . . . :   *SYSVAL
Programa de atención . . . . . :   USMAIN
  Biblioteca . . . . . :     TSAPUSU
Secuencia de ordenación  . . . . . :   *SYSVAL
  Biblioteca . . . . . :
Identificador de idioma  . . . . . :   *SYSVAL
Identificador de país o región . . . . . :   *SYSVAL
Identificador de juego de caracteres . . . :   *SYSVAL
Control de identificador de caracteres . . :   *SYSVAL
Atributos de trabajo de entorno nacional . :   *SYSVAL
Entorno nacional . . . . . :   *SYSVAL
Opciones usuario . . . . . :   *NONE
Valor de auditoría de objeto . . . . . :   *ALL
Valores de auditoría de acciones . . . . . :   *CMD
                                               *CREATE
                                               *DELETE
                                               *JOBDTA
                                               *OBJMGT
                                               *PGMADP
                                               *SAVRST
                                               *SECURITY
                                               *SERVICE
                                               *SPLFDTA
```

```
                                                *SYSMGT
Número de ID de usuario  . . . . . . . . . . :   1204
Número de ID de grupo  . . . . . . . . . . . :   *NONE
Directorio inicial . . . . . . . . . . . . . :   /home/SUPxxx
```

En el menú principal de los usuarios de este grupo se añade una opción para ejecutar comandos con este usuario especial. Esta opción escribirá en el registro de auditoría una entrada especial que indica que se ha realizado el cambio de usuario. La finalización de este cambio de usuario también será escrita en el registro. De este modo las herramientas de seguridad podrán monitorizar estos accesos “especiales” al sistema.

4.2.6. Usuarios de Software de Terceros

Los usuarios de software de terceros se utilizan principalmente para someter trabajos adoptando autorizaciones con estos usuarios y para acceder al menú de su aplicación. En medida de lo posible se debe eliminar el acceso a estos perfiles programando puertas de acceso, como en el modo del usuario EDITRAN que no permite iniciar sesión.

Aquellos usuarios de software de terceros que no se deban utilizar para someter trabajos (usuarios de instalación,...) deberán ser inhabilitados en cuanto dejen de utilizarse.

Por ser utilizados no pueden estar deshabilitados, pero se ponen a contraseña *NONE.

4.2.7. Usuarios del Sistema

Los usuarios que vienen definidos con el sistema operativo y los programas bajo licencia, deben ser inhabilitados y cambiada su contraseña, siempre que se pueda.

Se creará un documento en la base de datos de Sistemas en Lotus Notes con la relación de todos estos perfiles de usuario y sus contraseñas. Este documento deberá estar cifrado.

Se marcan como *DISABLED y con contraseña *NONE.

```
QAUTPROF
QBRMS
QCLUMGT
QCLUSTER
QCOLSRV
QDBSHR
QDBSHRDO
QDFTOWN
QDIRSRV
QDLFM
QDOC
QDSNX
QEJB
QEJBSVR
QFNC
QGATE
QIPP
QLPAUTO
QLPINSTALL
QMGTC
QMSF
QNETSPLF
QNFSANON
QNTP
QPEX
QPGMR
QPM400
QRJE
QRMTCAL
QSNADS
QSPL
QSPLJOB
QSRV
QSRVAGT
```

```
QSRVBAS
QSYS
QSYSOPR
QTCM
QTCP
QTFTP
QTIVOLI
QTIVROOT
QTIVUSER
QTMHHTP1
QTMHHTTP
QTMPLPD
QTSTRQS
QUSER
QYCMCIMOM
QYPSJSVR
```

5. Comunicaciones

5.1. Introducción

Las comunicaciones son uno de los puntos más delicados dentro de un sistema de seguridad, ya que los datos que están viajando deben ser asegurados en el transcurso de la operación de envío/recepción.

La confidencialidad y la integridad de los datos cuando viajan por canales de comunicaciones deben ser aseguradas ya que el riesgo de una intrusión en los sistemas auxiliares no controlables es mucho más probable.

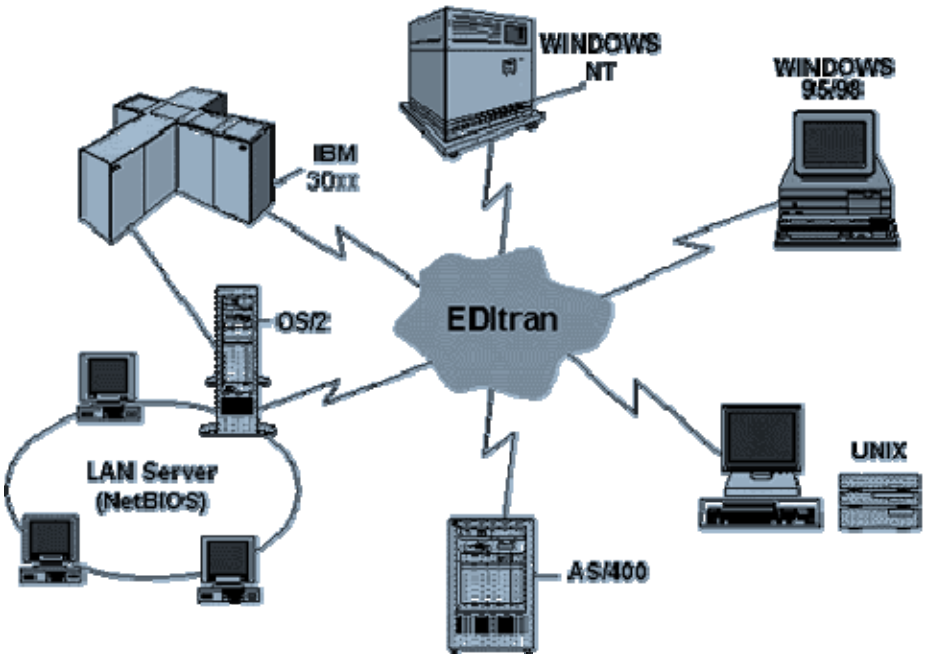
A su vez las redes de comunicaciones actúan con elementos intermediarios que almacenan y reenvían los datos de forma que se hace irremediablemente obligatorio aplicar medidas técnicas que garanticen la seguridad de éstos.

Es en este punto donde se realiza una de las recomendaciones más importantes de cara a salvaguardar la integridad, coherencia y confidencialidad de la información, dicha recomendación se fundamenta en la encriptación de los datos que viajan por la red mediante la ejecución del software EDITRAN; esto nos permitirá garantizar la seguridad de los envíos y recepciones.

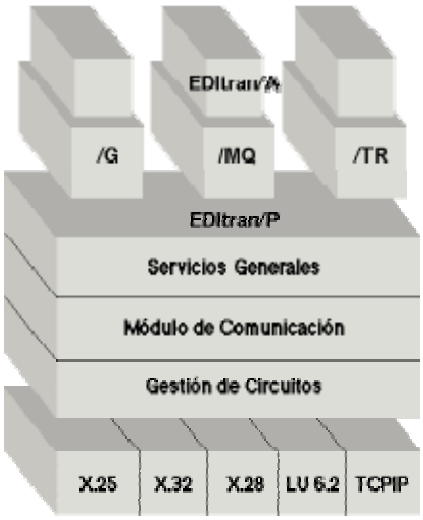
Otro de los aspectos de seguridad englobados dentro del capitulo de comunicaciones es el relativo al acceso a la información desde los puestos clientes mediante protocolos como FTP y ODBC, la ejecución de estos accesos sin control nos garantiza, antes o después, la inconsistencia de la información. Es por ello que se debe llevar a ejecución la recomendación realizada sobre el control de dichas acciones, siendo ésta ejecutada por el software POWERLOCK que nos permitirá restringir y controlar dichos accesos.

5.2. Software de transmisiones de datos: EDITRAN

La aplicación EDITRAN es un software proporcionado por la empresa INDRA para el intercambio de datos entre sistemas informáticos heterogéneos, pues permiten conectar la mayoría de las plataformas que se utilizan habitualmente para la implantación de los sistemas de comunicación.



La plataforma se estructura en los siguientes módulos:



Concretamente, en nuestro sistema utilizamos el módulo de EDItran/G y el módulo de EDItran/P. A grandes rasgos se pueden definir estos módulos como:

5.2.1. EDItran/P. Módulo de comunicaciones

Aporta a la plataforma el protocolo y los procedimientos de comunicaciones que han de ejecutarse en paralelo en los sistemas informáticos donde corren las aplicaciones usuarias de los sistemas de intercambios.

Permite la conectividad entre los sistemas informáticos heterogéneos, incorporando un protocolo de comunicación robusto que detecta las caídas de las líneas de transmisión, resincronizando automáticamente los envíos una vez subsanada la incidencia, a partir del punto en que se produjo la interrupción.

5.2.2. EDItran/G. Módulo de Gestión de Ficheros

Módulo que gestiona los intercambios de ficheros de datos, facilitando el acceso y la integración de los procesos de transmisión con los procesos de las aplicaciones usuarias, a las que aísla de la problemática de la presentación de los datos.

Prepara los ficheros de transmisión según los requerimientos del módulo de comunicaciones, realizando la compresión y cifrado de los datos en emisión, el descifrado y expansión de los datos recibidos, así como la generación de los diferentes ficheros planos de aplicación recibidos en las sesiones de transmisión.

Estos módulos se comunican con la máquina destino utilizando como medio la red pública de conmutación de paquetes Iberpac, a través de los servicios X.25

5.2.3. X.25

El X.25 es un estándar de la ITU-T ("*International Telecommunication Union - Telecommunication Standardization Sector*") para actuar como la interfaz entre un sistema y una red conmutada de paquetes. Se trata de un protocolo orientado a conexión, que presta una garantía de servicio. Permite gestionar una serie de eventos relativos a la conexión como pueden ser:

- Petición de llamada / llamada entrante
- Aceptación de llamada / comunicación establecida
- Solicitud de datos / indicación de datos
- Liberación de conexión / indicación de desconexión / confirmación de desconexión
- Asentimiento / control de flujo
- Reinicio/ rearranque / interrupción

5.2.4. Encriptación

Con la utilización de la criptografía es posible constituir redes privadas virtuales (VPNs) entre los sistemas informáticos de los actores de los sistemas EDI, lo que permite el intercambio confidencial y seguro de los datos, a través de las redes públicas de telecomunicación sin necesidad de constituir redes dedicadas, con el consiguiente ahorro de costes por la reutilización de los medios para distintos intercambios, con la correspondiente simplificación de los procedimientos de administración que se requerirían en el supuesto de utilizarse redes privadas reales, con líneas y medios estáticamente asignados.

De esta forma, se proporciona los servicios de seguridad necesarios para definir *criptosistemas de clave secreta*, también denominados *de claves simétricas*. La primera denominación es debida al carácter confidencial de la clave utilizada en el cifrado/descifrado de la información y la segunda porque la clave de cifrado coincide con la de descifrado; es decir, el descifrado de un texto encriptado ha de efectuarse con la misma clave que lo cifró (de ahí su carácter secreto).

Las Aplicaciones usuarias que definan un Sistema de Seguridad pueden utilizar diferentes servicios criptográficos para proteger la información que desean almacenar o bien intercambiar en redes de comunicación por canales inseguros. Para ello, cifran y descifran la información/datos utilizando una *clave de aplicación (*que, normalmente, cambian con cierta frecuencia) la cual, a su vez, cifran con otras *claves auxiliares* que se almacenan en ficheros de claves especialmente protegidos.

5.2.4.1. **El algoritmo de criptografía DES**

Las técnicas de criptografía que desarrolla, están basadas en el algoritmo estándar DES ("*Data Encryption Standard")*, también conocido como DEA "*DataEncryption Algorithm")* definido en ANSI X3.92-1981 e ISO 9372, en el modo de operación de cifrado en bloques CBC ("*Cipher Block Chaining")* definido en ANSI X3.106-1983 e ISO 8372.

Se trata del algoritmo más extendido para aplicaciones civiles de cifrado de datos y su utilización permite a las aplicaciones usuarias incorporar servicios de seguridad criptográfica tales como cifrado masivo de datos, autentificación de los extremos origen y destino, etc.

El algoritmo es simétrico, utiliza la misma clave para cifrar y descifrar, siendo el método de descifrado exactamente inverso del de cifrado, esto implica que al usar este algoritmo para cifrar ficheros a intercambiar entre dos organizaciones, la clave ha de acordarse entre los dos extremos implicados en el intercambio, debiéndose ser comunicadas la misma de uno a otro centro. Con frecuencia, es preciso, por tanto, implementar un sistema robusto y a la vez ágil de generación, gestión y notificación de las correspondientes claves privadas.

5.2.4.2. **Aspectos técnicos de la seguridad y riesgos.**

Las claves auxiliares se almacenan en el fichero interno del producto, así como la clave maestra. La clave maestra se utiliza para cifrar las claves auxiliares almacenadas en el fichero y para garantizar la seguridad del sistema hay que optar por un método de almacenamiento especial de la misma, para lo que se almacena de forma enmascarada en diferentes registros y posiciones aleatorias dentro del fichero de claves, para dificultar los ataques al sistema de seguridad a partir del descubrimiento de la clave de máxima jerarquía.

Las claves de aplicaciones se utilizan para el cifrado/descifrado de los datos de las aplicaciones cuya confidencialidad se quiere proteger. Han de almacenarse, cifradas bajo una clave auxiliar del fichero de claves, bien en memoria o en ficheros específicos de cada una y, por ello, también han de guardar el "label" de la correspondiente clave auxiliar. Su mantenimiento es responsabilidad exclusiva de la aplicación y, por tanto, no debe almacenarse en claro, para no violar la seguridad del sistema, ni cifrarla con la clave maestra, para no violar la integridad del sistema.

Dada la necesidad de que las claves deben ser compartidas entre el emisor y el receptor, existen dos modos de funcionamiento criptográfico:

- El modo de intercambio automático de claves. Este modo utiliza las claves criptográficas que EDITRAN intercambia de manera automática, es decir, los usuario no necesitan intercambiarse ninguna clave. En esta modalidad solo se soporta el algoritmo de cifrado DES de claves simétricas.

- El modo de intercambio externo de claves. Esta modalidad utiliza claves criptográficas que los usuarios deben haber intercambiado previamente por el método que estimen conveniente, concretamente en nuestro sistema, con un intercambio automático de claves estableciendo una sesión de modo coordinado entre los diferentes responsables de los sistemas. En esta modalidad se utiliza el algoritmo DES para el cifrado/descifrado de datos y el algoritmo DES o RSA, en nuestro caso el DES para ambos, para la autentificación de extremos y el intercambio de claves de sesión.

Esto nos permite aprovechar el modo automático para crear un procedimiento de intercambio de claves sencillo, pero a su vez seguro.

5.2.4.3. Procedimiento para el intercambio de claves

En primer lugar, tras haber creado la sesión, tanto en el equipo emisor como en el receptor, nos debemos poner en contacto con el operador de Editran de la entidad remota.

Ejemplo con la sesión PRUEBA.

```
EDITRAN P
  Opc. 3.- Administrador
    Opc. 2.- Sesiones
```

Seleccionamos PRUEBA para modificación.

```
Opción ......: M
Código Remoto: 0 0001234 0
Aplicación ..: PRUEBA
```

Accederemos a las opciones de criptografía, dejando el parámetro de cambio de clave en 'S'. Esto provocará que en la próxima conexión se envíe nuestra clave automáticamente al destino de la sesión. Si este cambio se realiza en ambos lados de la transmisión, se intercambiarán ambas claves.

```
                    Criptografía (S/N)  ..:    S
Versión Criptográfica .....:   220    Cambio de Clave V2.2 (S/N/U).: S
Algoritmo Confidencialidad.:   DES   Algoritmo Autenticación .....: DES
Clave Loc:                            Clave Rem:
```

Una vez cambiado el parámetro y tras haber confirmado que el otro extremo también lo ha cambiado, se realiza una petición de solicitud de sesión.

De este modo, se procederá al intercambio automático de claves.

```
Opc. 1.- Operador de editran

       Opción: 2
Código remoto: 0 0001234 0
   Aplicación: PRUEBA
```

Cuando se haya establecido la sesión correctamente, ya se puede liberar la sesión.

```
Opc. 3.- Petición de liberación de sesión
```

Una vez intercambiadas las claves volvemos a poner los parámetros de criptografía en su estado original.

```
                    Criptografía (S/N)  ..:    S
Versión Criptográfica .....:   220    Cambio de Clave V2.2 (S/N/U).: N
Algoritmo Confidencialidad.:          Algoritmo Autenticación .....: DES
Clave Loc:                            Clave Rem:
```

También se han de cambiar los parámetros de criptografía en EDItran/G dejándolos de la siguiente forma:

```
                  ---  Criptografía (S/N) : S  ---
Algoritmo Confidencialidad.: DES    Algoritmo Autentificación DES
Clave Loc:                          Clave Rem:
```

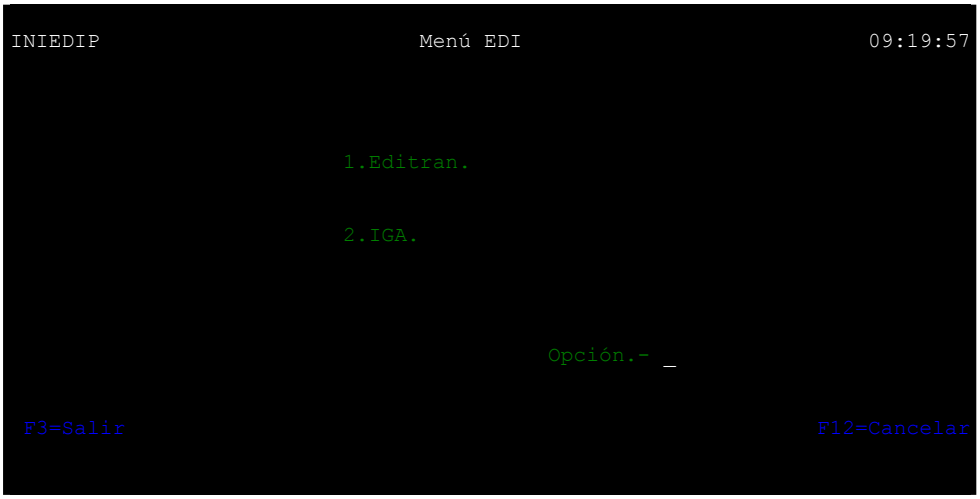
Tras este procedimiento, ambos lados de la transmisión habrán recibido, y enviado, las claves de las transmisiones, guardándolas para utilizarlas en las transmisiones.

5.2.4.4. Manual para dar de alta una sesión en EDITRAN

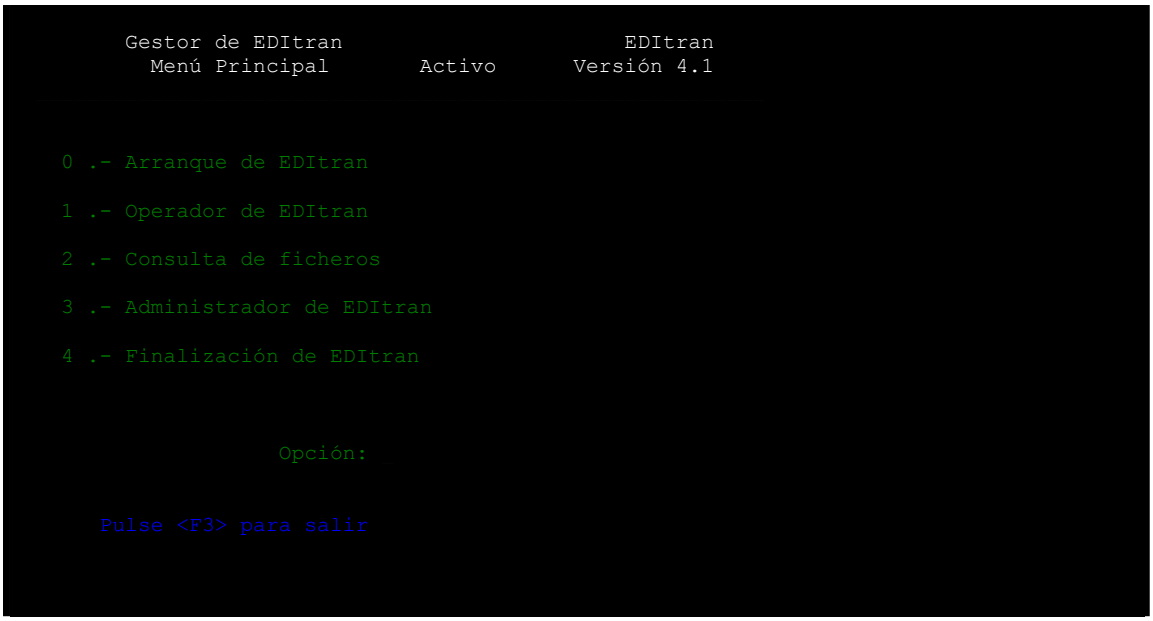
Para dar de alta una sesión Editran, es necesario darla de alta tanto en **EDItran/P** como **EDItran/G**.

A los menús de Editran, puede accederse llamando directamente al programa de editran (comando `EDITRAN` para editran p y comando `IGA` para editran G con el usuario Editran) pero el departamento de sistemas ha creado un menú de editran (pacoutl/edi) que permite acceder a los menús de editran sin necesidad de entrar con el usuario Editran (switch de usuario).

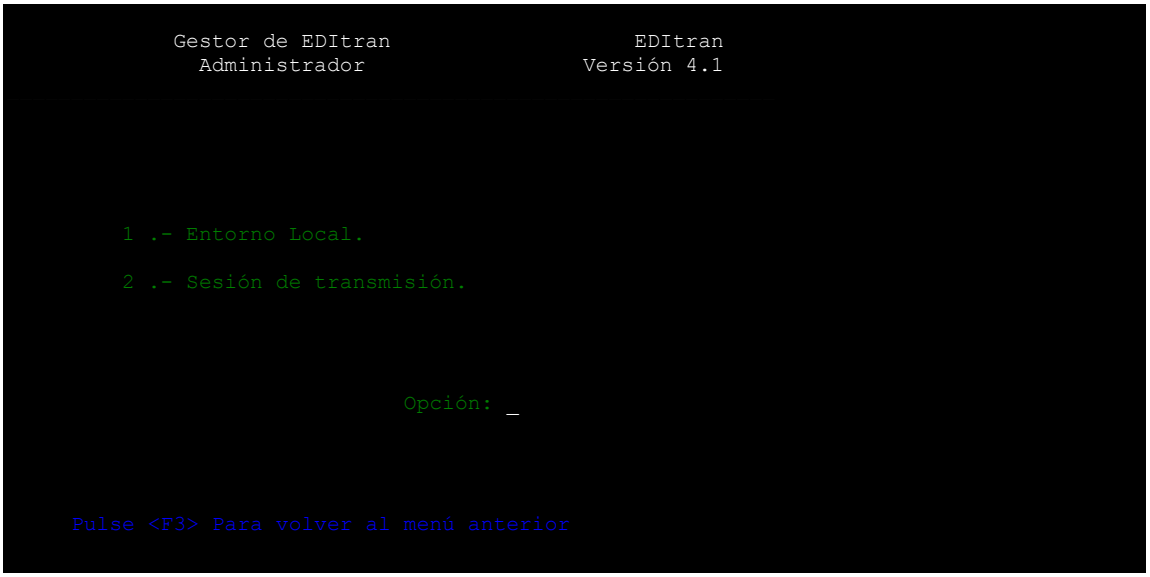
Por tanto, a la hora de dar de alta la sesión, llamar al menú de editran mediante: "**`PACOUTL/EDI`**"



Seleccionar la opción "1. **Editran"**



Seleccionar la opción “3. **Administrador de Editran”.**

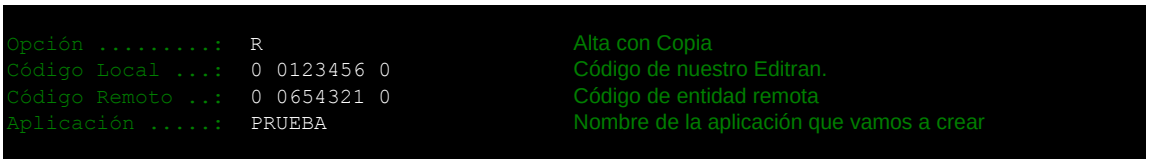


Seleccionar la opción “2. **Sesión de transmisión”.**

En esta pantalla se permite dar de alta, dar de baja, consultar, modificar o dar de alta mediante copia una sesión.

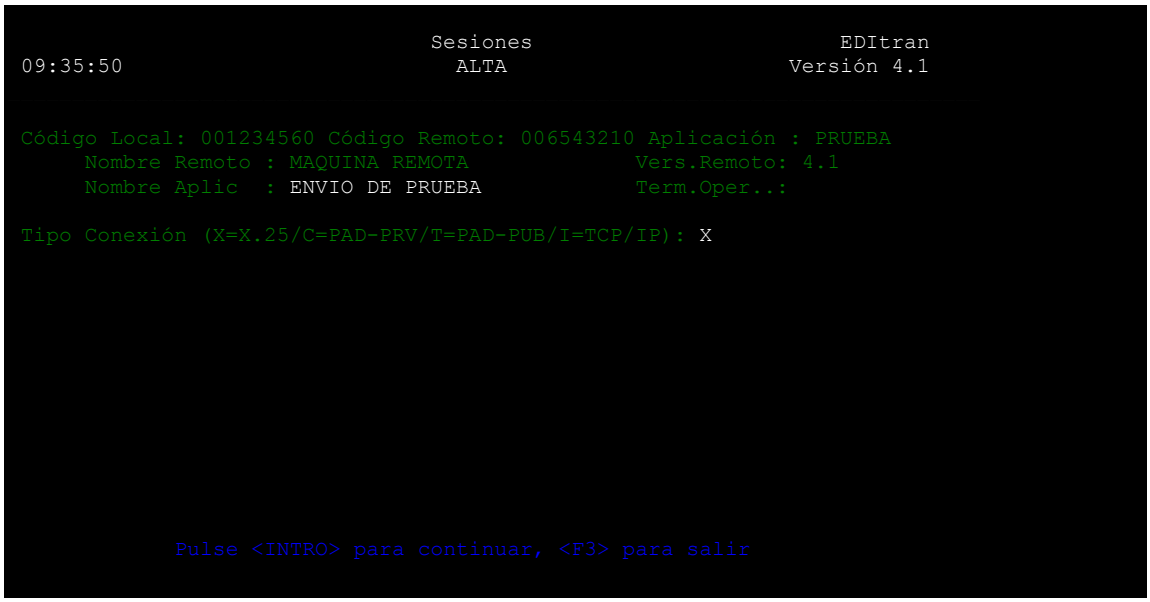
La opción que seleccionaremos es R para poder crear nuestra sesión como copia de otra y así evitar tener que introducir parámetros que son iguales para todas las sesiones.

Ejemplo:



Entonces nos pedirá la sesión de la que queremos copiar:

En la siguiente pantalla deberemos indicar que se trata de una transmisión a través de la línea X.25.

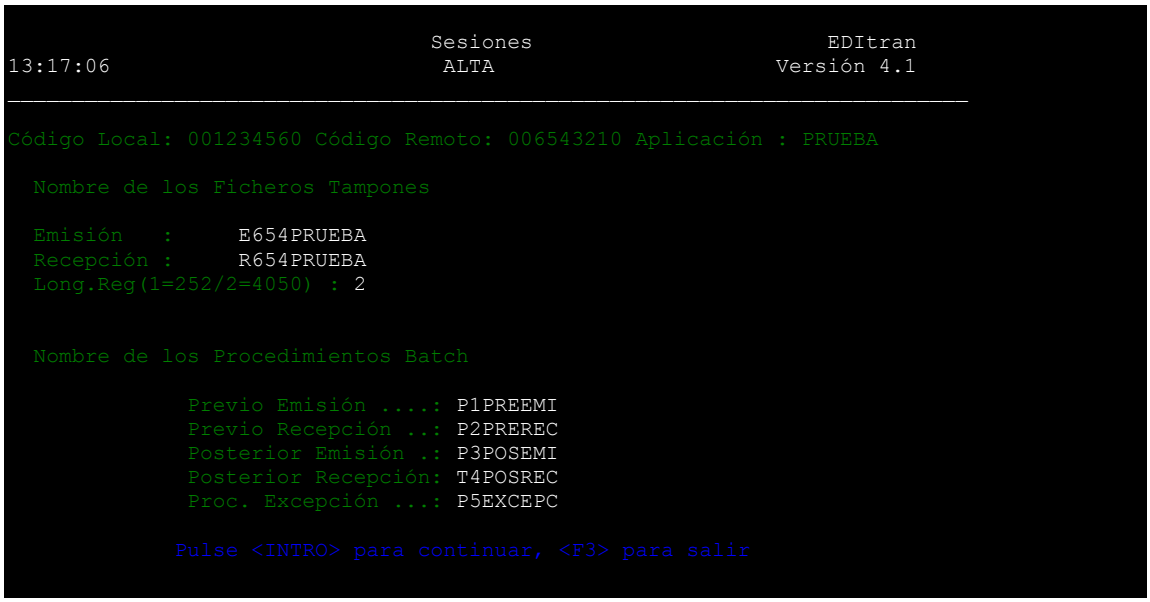


En "**Nombre Aplic**." se debe introducir una descripción de la nueva sesión.

En "**Tipo Conexión"** se indicará X (correspondiente a nuestra línea X.25).

Indicaremos el resto de los parámetros de conexión.

Y finalmente los parámetros internos de la aplicación.

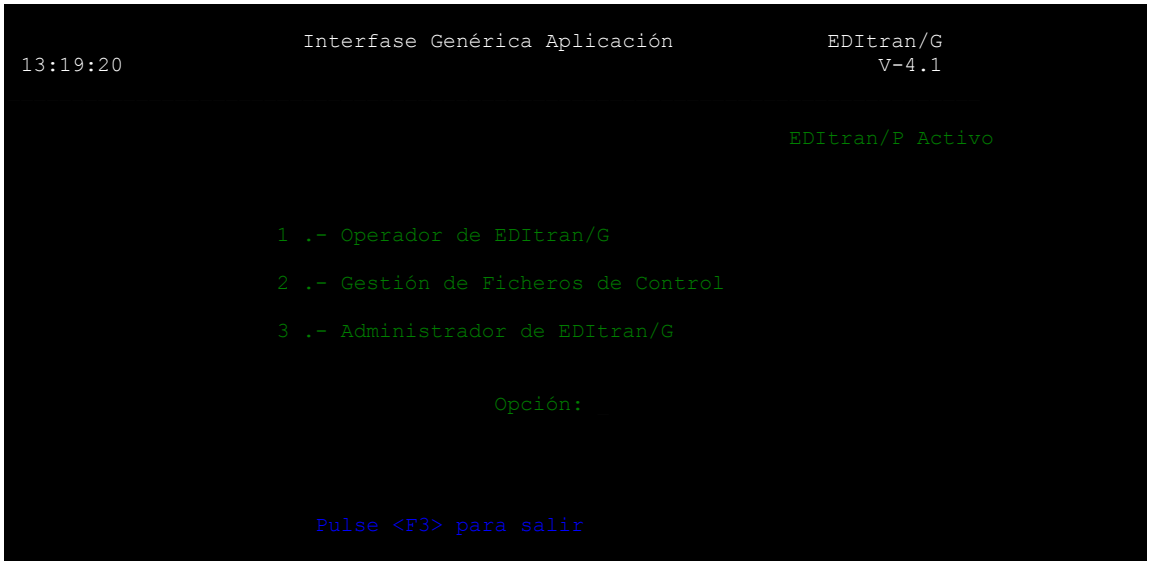


Revisaremos los tampones de emisión y recepción para que correspondan con la nomenclatura de la sesión.

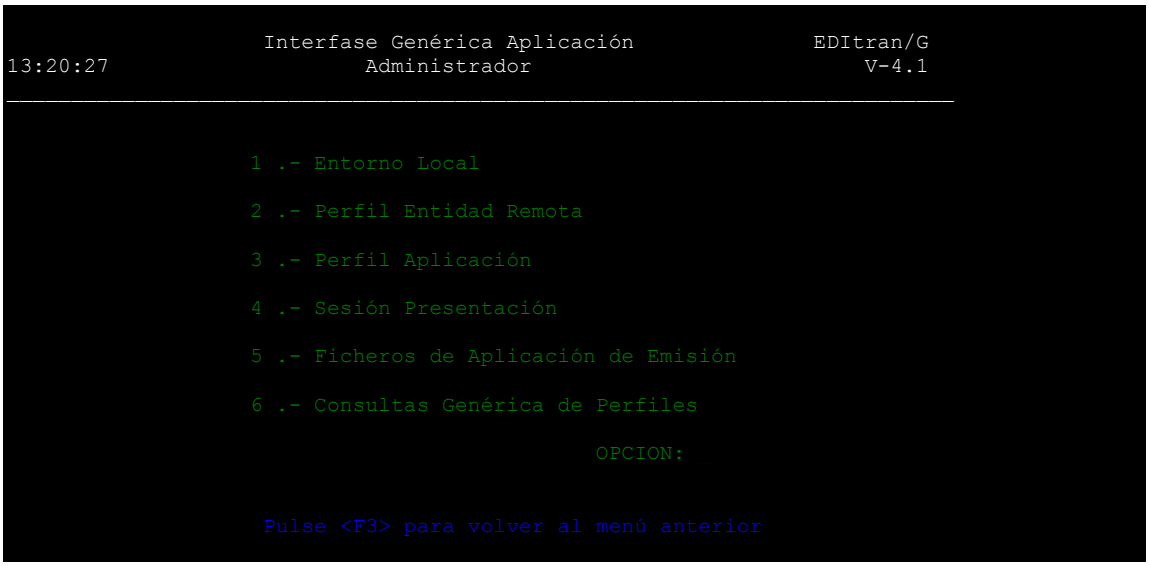
Y la longitud del registro debe ser “2” (que indica una longitud de 4050 caracteres).

Posteriormente daremos de alta la sesión en EDItran/G.

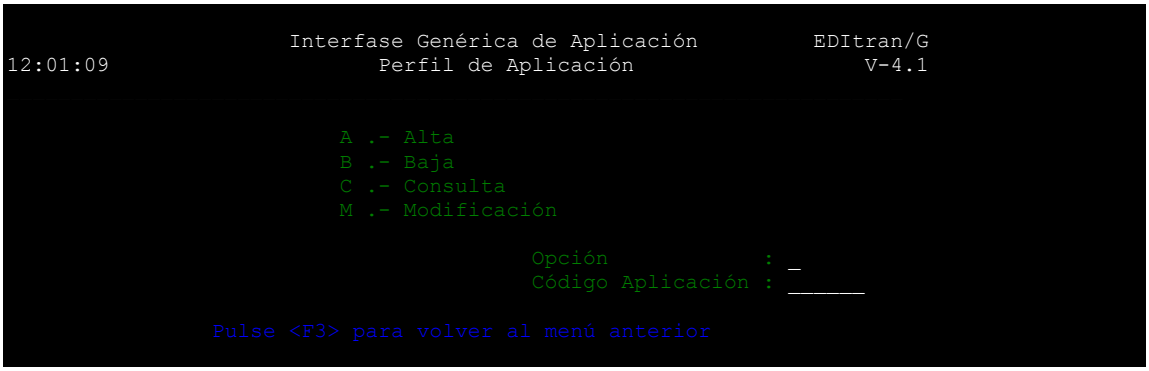
Seleccionar la opción “2. **IGA”.**



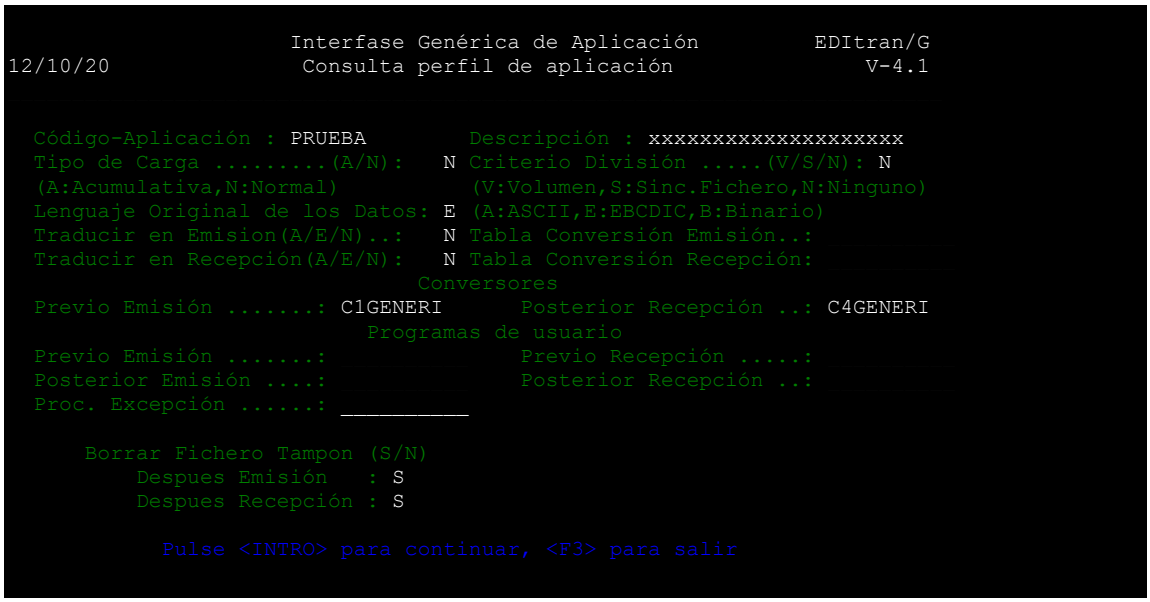
Seleccionar la opción “3. **Administrador de Editran/G”**



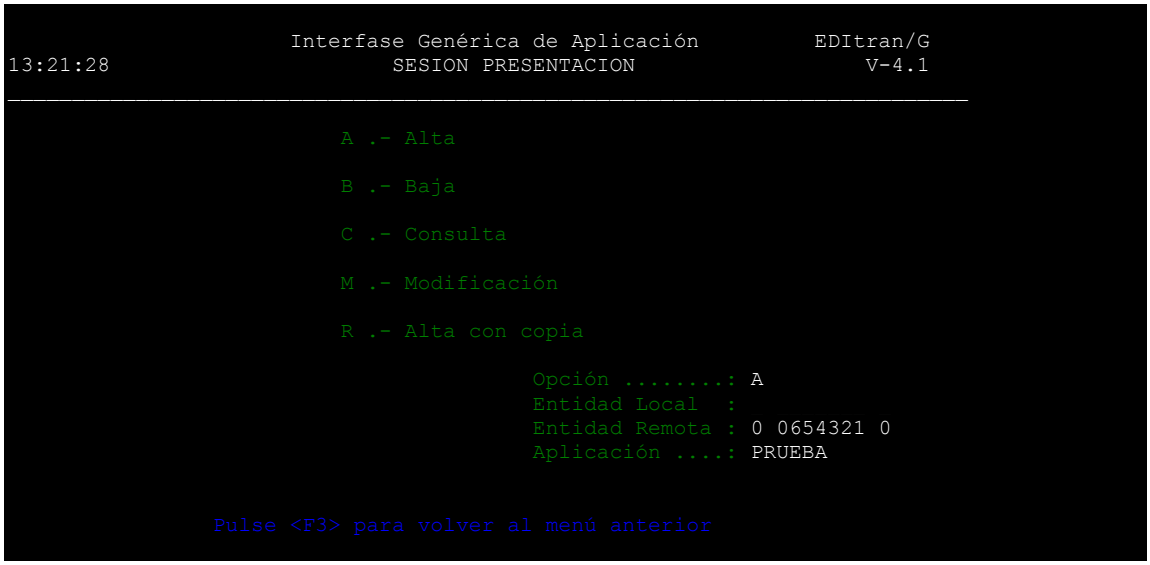
Seleccionar la opción 3. Perfil de aplicación:



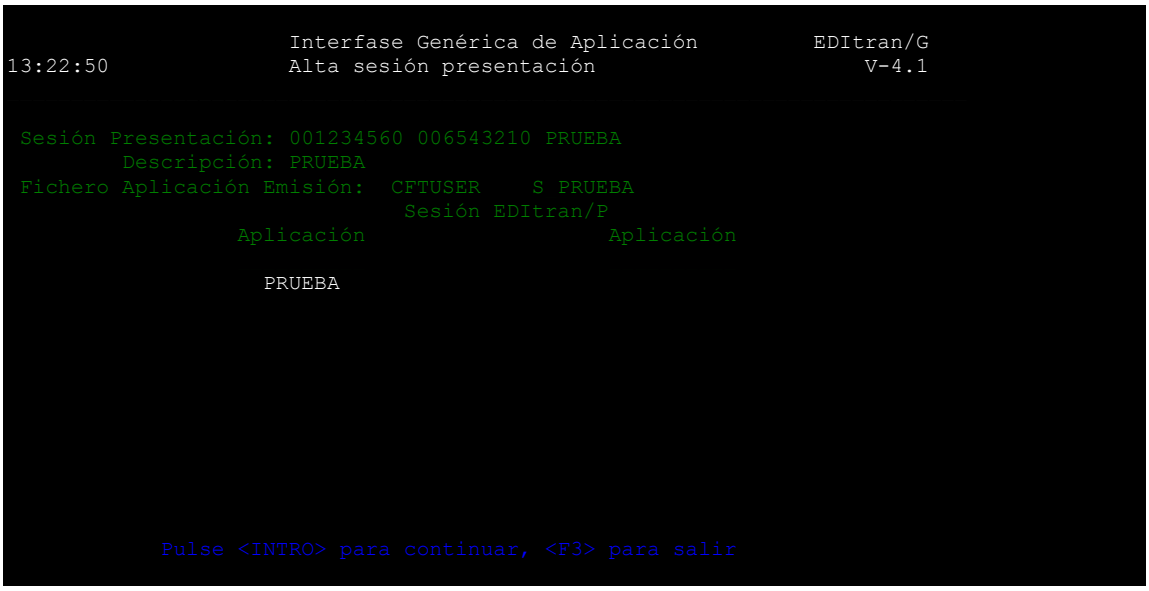
Seleccionar la opción A (Alta) y poner el nombre de la aplicación.



Volver al menú de IGA y seleccionar la opción 4. Sesión presentación

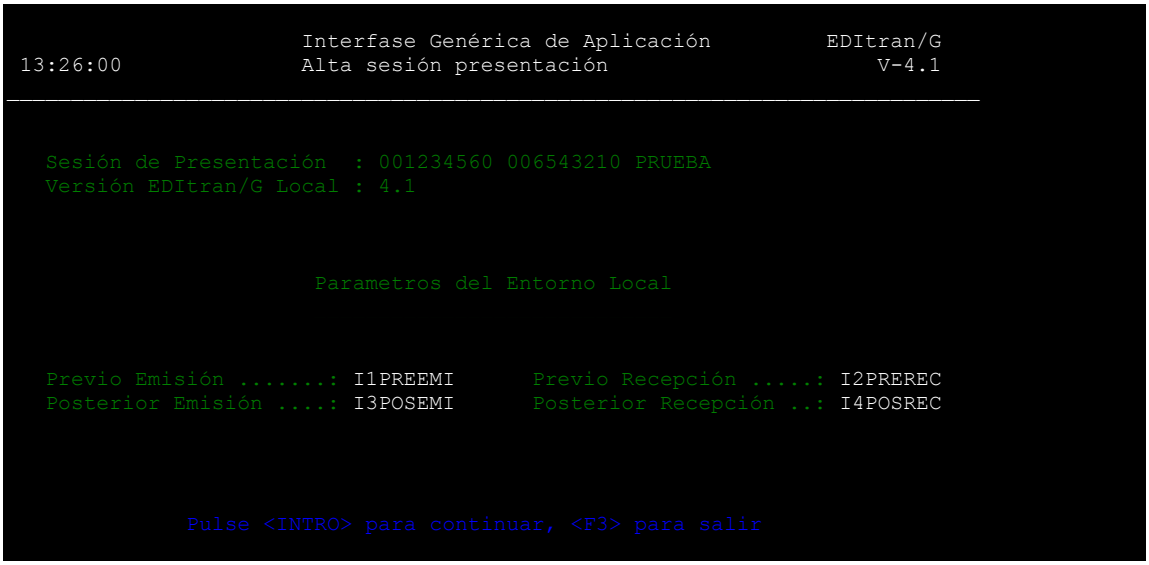


Seleccionar la opción **A** e indicar el nombre de la nueva sesión.



Se indica el nombre de la Aplicación (nombre de la sesión), biblioteca donde se encuentra el fichero a transmitir y nombre del fichero.

En caso de ser una sesión de recepción, no debe indicarse nada.



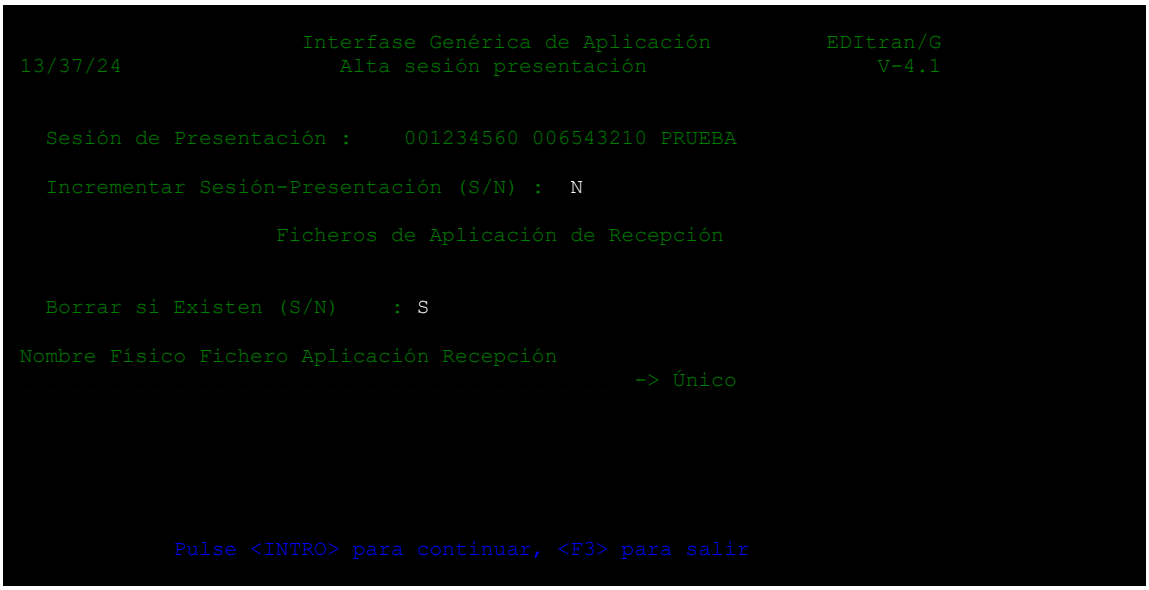
En esta pantalla no debe tocarse nada, son programas internos de editran.

```
                    Interfase Genérica de Aplicación        EDItran/G
13/27/26            Alta sesión presentación                    V-4.1


     Sesión de Presentación : 001234560 006543210 PRUEBA

                   Parametros de la entidad Remota

        Descripción ............:  MAQUINA REMOTA
        Versión EDItran/G Remota :  4.1
        Compresión (S/N) .......:  S
        Ascii/Ebcdic (A/E/B) ....:  E
        CRC (S/N) ..............:  N
                --  Seguridad de la Presentación  --
                ---  Criptografía (S/N) : N  ---
Algoritmo Confidencialidad.: ______ Algoritmo Autentificación: ______
Clave Loc:                          Clave Rem:

           Pulse <INTRO> para continuar, <F3> para salir
```

Indicaremos si la sesión lleva compresión y si es Ascii o Ebcdic. La parte de criptografía la dejamos a No.

```
                    Interfase Genérica de Aplicación        EDItran/G
13/29/59            Alta sesión presentación                    V-4.1
_____________________________________________________________________

  Sesión de Presentación : 001234560 006543210 PRUEBA
                       Parametros de la Aplicación
  Descripción: PRUEBA               Tipo de Carga (A/N): N (Acumul,Normal)
  Criterio División ............: N  (V:Volumen,S:Sinc.Fichero,N:Ninguno)
  Lenguaje Original de los Datos: E  (A:ASCII,E:EBCDIC,B:Binario)
  Traducir en Emision(A/E/N)..:   N  Tabla Conversión Emisión..:
  Traducir en Recepción(A/E/N):   N  Tabla Conversión Recepción:
                              Conversores
  Previo Emisión .......: C1GENERI      Posterior Recepción ..: C4GENERI
                            Programas de Usuario
  Previo Emisión .......: __________    Previo Recepción .....: __________
  Posterior Emisión ....:               Posterior Recepción ..:
  Proc. Excepción ......:

      Borrar Fichero Tampón (S/N)
          Despues Emisión   : S
          Despues Recepción : S
            Pulse <INTRO> para continuar, <F3> para salir
```

Indicamos los programas que se ejecutarán previo al envío, posterior al envío, previo a recepción, posterior a recepción. Se deberá rellenar los que procedan.



En caso de recepción, rellenar con la biblioteca en la que se desea recibir el fichero y el nombre del fichero.

5.3. POWERLOCK

A pesar de que los iSeries y las arquitecturas de seguridad del AS/400 son muy robustos, una mala configuración del sistema puede permitir que los usuarios finales puedan tener accesos no autorizados a los datos del sistema mediante herramientas como ODBC, FTP, DDM, etc. Sin embargo, el nivel de acceso que se puede controlar mediante los terminales no es el mismo que con los accesos externos, por ejemplo los permisos que necesita un usuario para ver los contenidos de un fichero en su cola de impresión son los mismos que los necesarios para bajar un fichero al PC y colgarlo en Internet.

Esta herramienta divide los accesos al servidor en diferentes tipos, al mismo tiempo que cada tipo se divide en sus correspondientes funciones:

- *CLI → Servicio de conexión
  - CONNECT → Conexión
- *CNTRLSRV → Servidor central de gestión de licencias
  - RLSLIC → Eliminar licencia
  - RQSLIC → Solicitar licencia
  - RTVCNVMAP → Obtener mapa de conversión
  - RTVLICINF → Recuperar información de licencia
  - SETACT → Activar cliente
  - SETINACT → Desactivar cliente
- *DATAQSRV → Servidor optimizado de colas de datos
  - CLRDTQMSG → Borrar mensajes de una cola de datos
  - CNLPNDRCV → Cancelar solicitud de colas de datos
  - CRTDTQ → Crear una cola de datos
  - DLTDTQ → Borrar una cola de datos
  - QRYDTQATR → Obtener las propiedades de las colas de datos
  - RCVDTQMSG → Recibir mensajes de la cola de datos
  - RECVMSG → Recibir mensajes de datos
  - SNDDTQMSG → Enviar un mensaje a la cola de datos

- *DDM → Servicio de conexiones DDM
  - ADDMBR → DDM añadir miembro
  - CHANGE → DDM modificar datos
  - CHGDTAARA → DDM Cambiar area de datos
  - CHGMBR → DDM cambiar miembro
  - CLEAR → DDM Limpiar
  - CLRDTAQ → DDM Limpiar cola de datos
  - COMMAND → DDM Comando remoto
  - COPY → DDM Copiar
  - CREATE → DDM Crear
  - DELETE → DDM Borrar
  - EXTRACT → DDM Extraer
  - INITIALIZE → DDM Inicializar
  - LOAD → DDM Cargar
  - LOCK → DDM Bloquear
  - MOVE → DDM Mover
  - OPEN → DDM Abrir
  - RCVDTAQ → DDM Recibir cola de datos
  - RENAME → DDM Renombrar
  - RGZMBR → DDM Reorganizar miembro
  - RMVMBR → DDM Borrar miembro
  - RNMMBR → DDM Renombrar miembro
  - RTVDTAARA → Obtener area de datos
  - SNDDTAQ → Enviar cola de datos
  - UNLOAD → DDM Descargar
- *DQSRV → Servidor de colas de datos
  - CLEAR → Borrar mensajes de una cola de datos
  - CREATE → Crear una cola de datos
  - DELETE → Borrar una cola de datos
  - PEEK → Visualizar cola de datos
  - QUERY → Consultar una cola de datos
  - RECEIVE → Recibir un mensaje de una cola de datos
  - SEND → Enviar un mensaje a una cola de datos
- *DRDA → Base de datos relacional distribuida

    - SQLCNN → Conexión SQL
- *FILESRV → Servidor de ficheros
    - ALCSTRMCNV → Obtener comunicación
    - CHGSTRMATR → Cambiar los atributos de un fichero
    - CRTSTRMFIL → Crear un fichero o directorio
    - DLTSTRMFIL → Borrar un fichero o directorio
    - LSTSTRMATR →Ver los atributos de un fichero
    - MOVSTRMFIL → Mover fichero
    - OPNSTRMFIL → Abrir fichero
    - RNMSTRMFIL → Renombrar fichero
- *FTPCLIENT → Cliente FTP de iSeries
    - CHGCURLIB → Cambiar la biblioteca actual (LCD)
    - INIT → Iniciar sesión (OPEN)
    - RECVFILE → Obtener fichero (GET, MGET)
    - RMTCMD → Ejecutar comando remoto (SYSCMD)
    - SENDFILE → Enviar fichero (APPEND, PUT, MPUT)
- *FTPREXEC → Ejecución de comandos remotos FTP (REXEC)
    - INIT → Iniciar sesión
    - RMTCMD → Ejecutar comando remoto
- *FTPSERVER → Servidor FTP iSeries
    - CHGCURLIB → Cambiar la biblioteca actual (CD,CDUP,XCD,XCUD)
    - CREATELIB → Crear una biblioteca (MD,MKD,XMKD)
    - DELETEFILE → Borrar ficheros (DELE)
    - DELETELIB → Borrar bibliotecas (RMD,XRMD)
    - INIT → Iniciar sesión
    - LISTFILES → Obtener listado de ficheros en directorio (LIST,NLIST)
    - RECVFILE → Recibir un fichero (APPE,STOR,STOU)
    - RMTCMD → Ejecutar comando remoto
    - RNMFILE → Renombrar fichero (RNFR, RNTO)
    - SENDFILE → Enviar fichero (RETR)
- *FTPSIGNON → Servicio FTP de inicio de sesión

- SIGNON → Iniciar sesión FTP

- *LMSRV → Servidor gestor de licencias
  - RELEASE → Eliminar licencia
  - REQUEST → Solicitar licencia
- *MSGFCL → Servicio de mensajes
  - RECEIVE → Recibir mensaje
  - SEND → Enviar mensaje
- *NDB →Peticiones de bases de datos nativas
  - ADDDBFMBR → Añadir miembro a una base de datos
  - ADDLIBL → Añadir biblioteca
  - CLRDBFMBR → Borrar datos de un miembro
  - CRTDBF → Crear fichero de base de datos
  - CRTSRCPF → Crear fichero de fuentes
  - DLTDBFMBR → Borrar miembro de base de datos
  - DLTDBFOVR → Borrar mascara de un fichero
  - DLTF → Borrar fichero
  - OVRDBF → Enmascarar fichero
- *REXEC_SO → Servicio de ejecución remota en el inicio de sesión
  - SIGNON → Ejecutar un comando
- *RMTSRV → Servidor de comandos remoto
  - DSTPGMCALL → Llamada a un programa distribuido
  - RMTCMD → Ejecutar comando remoto
- *RQSRV → Servidor remoto de SQL
  - CONNECT → Conectar a una base de datos
  - CREATEPKG → Crear un paquete SQL
  - DELETE → Borrar Delete fila
  - EXECPKG → Ejecutar commando SQL empaquetado (no SELECT)
  - EXECUTE → Ejecutar commando SQL (no SELECT)
  - EXECUTEPM → Ejecutar SQL (no SELECT) con parametros
  - PREPTOPKG → Preparar commando SQL en un paquete

- RMTCALL → Ejecutar programa de AS400
- SELECT → Seleccionar filas
- SELECTPKG → Abrir un commando SELECT almacenado
- SELECTPM → Preparar un commando SELECT con parámetros
- SELECTVAL → Preparar un commando SELECT empaquetado con parametros
- UPDATE → Actualizar columnas

- *RTVOBJINF → Servicio de obtención de información de objetos SQL
  - RTVCLMINF → Obtener información especial de columa
  - RTVFILINF → Obtener información de fichero
  - RTVFKEYINF → Obtener información de clave ajena
  - RTVFLDINF → Obtener información de los campos
  - RTVFMTINF → Obtener información del formato de los registros
  - RTVIDXINF → Obtener información de los índices
  - RTVLIBINF → Obtener información de la biblioteca
  - RTVMBRINF → Obtener información de los miembros de un fichero
  - RTVPKEYINF → Obtener inforamción de la clave primaria
  - RTVRDBINF → Obtener información de la base de datos
  - RTVSQLPKG → Obtener información de los paquetes SQL
  - RTVSQLSTMT → Obtener información de la sentencia SQL
- *SIGNON → Servicio de inicio de sesión
  - CHGPWD → Cambiar clave
  - RETRIEVE → Obtener información de inicio de sesión
- *SQL → Servidor de bases de datos
  - INIT → Inciar SQL
- *SQLSRV → Servidor SQL
  - CLEARPKG → Limpiar paquete
  - CONNECT → Conectar
  - CREATEPKG → Crear paquete

    - DELETEPKG → Borrar paquete
    - EXECOPEN → Ejecutar o abrir
    - EXECUTE → Ejecutar
    - EXECUTEIMM → Ejecutar inmediatamente
    - FETCH → Obtener un stream
    - OPEN → Abrir
    - OPENFETCH → Abrir y obtener un stream
    - PREPARE → Preparar
    - PRPDESCRB → Preparar y definir
    - PRPEXECUTE → Preparar y ejecutar
- *TELNET → Servidor Telnet
    - INIT → Iniciar dispositivo Telnet
- *TFRFCL → Servidor de transferencia de ficheros
    - EXTRACT → Obtener un listado de comandos
    - JOIN → Obtener fichero del AS/400 y volcar en fichero existente
    - REPLACE → Enviar fichero al AS/400 sobreescribiendo
    - SELECT → Obtener fichero del AS/400
- *TFTP → Servidor Trivial FTP
    - RECVFILE → Recibir fichero
    - SENDFILE → Enviar fichero
- *VISTA → Servidor ShowCase *VISTA
    - DELETE → ShowCase Vista DELETE
    - GRANT → ShowCase Vista GRANT
    - INSERT → ShowCase Vista INSERT
    - JOIN → ShowCase Vista JOIN
    - REVOKE → ShowCase Vista REVOKE
    - SELECT → ShowCase Vista SELECT
    - UPDATE → ShowCase Vista UPDATE
- *VISTAPRO → Servidor ShowCase *VISTAPRO
    - DELETE → ShowCase *VISTAPRO DELETE
    - GRANT → ShowCase *VISTAPRO GRANT
    - INSERT → ShowCase *VISTAPRO INSERT

    - JOIN → ShowCase *VISTAPRO JOIN
    - REVOKE → ShowCase *VISTAPRO REVOKE
    - SELECT → ShowCase *VISTAPRO SELECT
    - UPDATE → ShowCase *VISTAPRO UPDATE
- *VPRT → Servidor virtual de impresión
    - CHECK → Comprobar permisos de impresión
    - EXTRACT → Obtener una lista de funciones
    - OPEN → Abrir fichero de impresión
- *WSG → Servidor Gateway de las estaciones de trabajo
    - SIGNON → Iniciar sesión
- ANALYZER → Servidor ShowCase Analyzer
    - DELETE → ShowCase Analyzer DELETE
    - GRANT → ShowCase Analyzer GRANT
    - INSERT → ShowCase Analyzer INSERT
    - JOIN → ShowCase Analyzer JOIN
    - REVOKE → ShowCase Analyzer REVOKE
    - SELECT → ShowCase Analyzer SELECT
    - UPDATE → ShowCase Analyzer UPDATE
- DATA_VIEW → Servidor ShowCase DATA_VIEW
    - DELETE → ShowCase Data_View DELETE
    - GRANT → ShowCase Data_View GRANT
    - INSERT → ShowCase Data_View INSERT
    - JOIN → ShowCase Data_View JOIN
    - REVOKE → ShowCase Data_View REVOKE
    - SELECT → ShowCase Data_View SELECT
    - UPDATE → ShowCase Data_View UPDATE
- DATADIST → Servidor ShowCase DATADIST
    - ALTER → ShowCase Data Dist ALTER
    - CREATE → ShowCase Data Dist CREATE
    - DELETE → ShowCase Data Dist DELETE
    - DROP → ShowCase Data Dist Drop
    - GRANT → ShowCase Data Dist GRANT
    - INSERT → ShowCase Data Dist INSERT

  - JOIN → ShowCase Data Dist JOIN
  - LABEL → ShowCase Data Dist LABEL
  - REVOKE → ShowCase Data Dist REVOKE
  - SELECT → ShowCase Data Dist SELECT
  - UPDATE → ShowCase Data Dist UPDATE
- INFO_DIR_W → Servidor ShowCase INFO_DIR_W
  - JOIN → ShowCase INFO_DIR_W JOIN
- QNPSERVR → Servidor de impresión en red
  - INIT → Iniciar servidor de impresión
  - PROCESS → Procesar un fichero de salida de impresión
- VISTA_ADMI → Servidor ShowCase VISTA_ADMI
  - DELETE → ShowCase Vista_Admi DELETE
  - GRANT → ShowCase Vista_Admi GRANT
  - INSERT → ShowCase Vista_Admi INSERT
  - JOIN → ShowCase Vista_Admi JOIN
  - REVOKE → ShowCase Vista_Admi REVOKE
  - SELECT → ShowCase Vista_Admi SELECT
  - UPDATE → ShowCase Vista_Admi UPDATE

En nuestro caso, y tras estudiar el tipo de accesos externos que se realizan, se definen una serie de servicios y funciones como restringidas:

- ***TFRFCL**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.
Funciones restringidas: *EXTRACT, SELECT, JOIN y REPLACE

- ***RTVOBJINF**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.
Funciones restringidas: TODAS.

- ***NDB**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: TODAS.

- ***SQLSRV**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: TODAS.

- ***FTPSIGNON**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: SIGNON.

- ***FTPCLIENT**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: INIT, CHGCURLIB, SENDFILE, RECVFILE, RMTCMD

- ***FTPSERVER**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: INIT, CHGCURLIB, DELETELIB, CREATELIB, LISTFILES, DELETEFILE, SENDFILE, RECVFILE, RNMFILE, RMTCMD

- ***TFTP**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: RECVFILE, SENDFILE

- ***FLSRV**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.

Funciones restringidas: ALCSTRMNCV, CRTSTRMFIL, DLTSTRMVIL, TNMSTRMFIL, LSTSTRMATR, CHGSTRMATR, MOVSTRMFIL, OPNSTRMFIL

- ***RMTSRV**

Usuarios: EXPLOT, MANTEN, INSTAL, DESCONS. (A TSISTEMAS se le permite ya que es necesario para entrar en iseries Navigator)

Funciones restringidas: TODAS

- ***FTPREXEC**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.
Funciones restringidas: TODAS

- ***RQSRV**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.
Funciones restringidas: *ALL

- ***SQL**

Usuarios: TSISTEMAS, EXPLOT, MANTEN, INSTAL, DESCONS.
Funciones restringidas: TODAS

- ***VPRT**

Usuarios: TODOS.
Funciones restringidas: TODAS

- ***QNPSERVR**

Usuarios: TODOS.
Funciones restringidas: TODAS

- ***DQSRV**

Usuarios: TODOS.
Funciones restringidas: TODAS

- ***DATAQSRV**

Usuarios: TODOS.
Funciones restringidas: TODAS

- ***WSG**

Usuarios: TODOS.
Funciones restringidas: TODAS

- ***MSGFCL**

Usuarios: TODOS.

Funciones restringidas: TODAS

6. Sistema de Backup

6.1. Introducción

Dos importantes recomendaciones realizadas son la creación de procedimientos para la restauración guiada del sistema y la restauración de datos mediante el BRMS.

En caso de un restaurado total del sistema, depender de la habilidad del personal que la realiza puede ser muy peligroso. Un paso mal ejecutado u omitido puede llevar a una situación muy compleja de resolver, pudiendo necesitar, en caso extremo, volver a repetir el proceso duplicando, de este modo, la cantidad de tiempo necesaria para volver a la situación inicial.

En un caso menos crítico, aunque también delicado, se requiere de un procedimiento que marque el modo de restaurado habitual de unos objetos, se puede prevenir que existan casos en los que al restaurar erróneamente un objeto se pueda trabajar con información equivocada.

6.2. Creación de un procedimiento guiado de restauración del sistema.

Al procedimiento paso a paso, se han añadido campos para anotar las observaciones que se puedan considerar importantes, y unos campos en los que se puede anotar la hora de ejecución y duraciones. Esto nos permite evolucionar el siguiente procedimiento en las diferentes pruebas de contingencias para que sea lo más útil posible. Tanto para anotar posibles detalles a tener en cuenta o a estudiar más adelante, como para tener un cálculo de tiempos que se necesitan para devolver la máquina al estado original en caso de contingencia real.

Acción	Observaciones	Hora	T.Total	Fin Ok
Restaurar LIC – Con salvado mensual -				
Montar cartucho con salvado total en medio de IPL alternativo.	Si fallara la restauración del LIC instalarlo desde CDs			
Verificar la contraseña DST de QSECOFR				
Hacer IPL manual desde IPL alternativo - Desde panel poner modo manual. - Con botón Function Select poner 02 (IPL) en display. - Pulsar Enter. - Con botón Function Select poner D (IPL from tape o CD ROM) . - Pulsar Enter. Si el sistema se apaga. Encenderlo y pasar al siguiente paso. Si el sistema NO se apaga. -Seleccionar 3 (continuar con IPL) en el display. -Pulsar Enter.				
Pantalla Install Licensed Internal Code Opción 1. Install Licensed Internal Code				
Pant. Install Licensed Internal Code (LIC)				

Opción 2, Install Licensed Internal Code and Initialize System				
F10 para confirmar instalación.				
Pantalla Initialize the Disk - Status				
Pantalla Install Licensed Internal Code - Status				
Pantalla Disk Configuration Attention Report. Pulsar F10 para aceptar problemas y continuar.				
Pantalla IPL or Install the System Opción 3. Use Dedicated Service Tools (DST)				
Pantalla DST Login como QSECOFR QSECOFR				
Option 4, Work with Disk Units				
Option 1, Work with Disk Configuration				
Option 3, Work with ASP Configuration				
Option 3, Add Units to ASPs				
Pant. Specify ASPs to Add Units to 1 por cada unidad que hay que añadir al System ASP (ASP 1) + Enter				
Pantalla confirmación. Enter				
Pantalla Problem Report Pulsar F10				
Pantalla Function Status Muestra % Después de mensaje “Selected units have been added successfully.” Pulsar F12				
Pantalla Work with Disk Configuration pulsar F3 hasta Exit Dedicated Service Tools (DST)				
Opción 1 Exit DST.				

Acción	Observaciones	Hora	T.Total	Fin Ok.
Pantalla IPL or Install the System screen 3, Use Dedicated Service Tools (DST)				
Login en DST con QSECOFR QSECOFR				
Pantalla Use Dedicated Service Tools (DST) 5, Work with DST environment				
Pantalla DST Environment 2, System Devices				
Pantalla System Devices 6, Console Mode				
Pantalla Select Console Type 2, Operations Console				
Pulsar F3 ó F12				

Acción	Observaciones	Hora	T.Total	Fin Ok
Restaurar S.O. – Desde el salvado mensual -				
Pantalla IPL or Install the System 2, Install the Operating System				
Pantalla Confirm Install of OS/400® Enter				
Pantalla Select a Language Group Verificar lenguaje primario y pulsar enter.				
Pantalla Add All Disk Units to the System Opción 1. Keep the current disk configuration	Para mantener la configuración actual de disco.			
Pantalla Install the Operating System Corregir fecha y hora si es necesario. Opción 2 "Change install options".	Esta opción se ha de seleccionar si se está restaurando en un sistema distinto de donde se salvó. De esta forma restaura nuestros atributos de red a partir del salvado.			
Pantalla Specify Install Options Poner los siguientes valores: Restore option.1 Job and output queues option .2				
Pantalla "Specify Restore Options" Poner 1 en todos los campos.				
Pantalla “Installation Status” ...progreso de la instalación...				
Pantalla de inicio. Hacer login con QSECOFR. NO es necesaria contraseña.				
Pantalla “IPL Options” Poner valores de fecha y hora. Poner Y sólo en las tres últimas opciones.				

Start system to restricted state . . . . . Y Set major system options . . . . . Y Define or change system at IPL . . . . Y				
Pantalla Set Major System Options Enable automatic configuration..: Y				
Pantalla Define or Change the System at IPL 3, System Value Commands				
Pantalla Change System Value Commands 3, Work with System Values				
Pantalla Work with System Values Anotar valor actual y cambiar los siguientes valores del sistema: QALWOBJRST to *ALL QJOBMSGQFL to *PRTWRAP QJOBMSGQMX size to a minimum value of 30 QPFRADJ to 2 QVFYOBJRST = 1 QCRTAUT=*USE QINACTITV=*NONE Pulsar ENTER F3 dos veces.	Comprobar si es necesario cambiar algún otro valor.			
Pantalla Define or Change the System at IPL F3 para salir y continuar con el IPL				
Pantalla Change Password Poner QSECOFR como contraseña actual y cambiarla --> Apuntarla aquí ---------->				

Acción	Observaciones	Hora	T.Total	Fin Ok
Pantalla: Menú principal del AS400. WRKRPYLE y comprobar si existe una entrada para CPA3709. Si no es así pulsar F6 y añadir la siguiente entrada: MSGID(CPA3709) RPY(G) Pulsar F5 y comprobar que se ha añadido correctamente.				
CHGJOB INQMSGRPY(*SYSRPYL) para actualizar el trabajo actual y que use la lista de respuestas modificada.				
Crear usuario USUARIO (pwd USUARIO1) copia de QSECOFR				

Acción	Observaciones	Hora	T.Total	Fin Ok
En este punto habría que ir al menú RESTORE y usar la opción 21, pero para el correcto funcionamiento de BRMS deben hacerse los mandatos uno a uno, para poder separar *IBM de *ALLUSR.				
ENDSBS SBS(*ALL)				
OPTION(*IMMED)				
RSTUSRPRF USRPRF(*ALL) ALWOBJDIF(*ALL)	Al terminar cada restaurado DSPJOBLOG a *PRINT.			
RSTCFG OBJ(*ALL) ALWOBJDIF(*ALL) SRM(*NONE)				
El parámetro SRM debe llevar *NONE para evitar que restaure la configuración de hardware del sistema original.	Al terminar cada restaurado DSPJOBLOG a *PRINT.			
RSTLIB SAVLIB(*IBM) ALWOBJDIF(*ALL) OMITLIB(Q1ABRMSF Q1ABRMSF01 QUSRBRM QBRM)				
RSTLIB SAVLIB(*ALLUSR) ALWOBJDIF(*ALL) OMIT(ACMSRCTL ACMSRLIB AISTOOLS AUDITORIA AUXPAQ AVP CFTPGM1 CFTPROD1 CFTUSER CGAPP CGDATA CGGL CGINSTAL CGSG CRIPTDES CRIPTRSA				

EDITRAN41 IMPRPRIMP OPNSSEG OPNSPEN PACOUTL POWERLOCK POWER471 PPOBJ	Al terminar cada restaurado DSPJOBLOG a *PRINT. ¡¡Asegurarse del nombre del dispositivo es mayús ó minús)!!			
PPSRC Q1ABRMSF Q1ABRMSF01 QUSRBRM QBRM SEC2077 ZIPAVF ZIPPPDAT) RSTDLO DLO(*ALL) SAVFLR(*ANY) ALWOBJDIF(*ALL) RST DEV('/QSYS.LIB/TAP01.DEVD') OBJ(('/*') ('/QSYS.LIB' *OMIT) ('/QDLS' *OMIT)) ALWOBJDIF(*ALL) RSTAUT (restaurar autorizaciones)	Si da errores RSTAUT buscar CPFs listados al final del documento.			

Acción	Observaciones	Hora	T.Total	Fin Ok
Configuración TCP/IP y líneas				
ENDTCP				
Desactivar línea LINDIRECTA WRKLIND LINDIRECTA Opc. 8, 2				
WRKHDWRSC *CMN	Anotar el nombre del dispositivo 2838 . Anotar el nombre del dispositivo 2745. .			
WRKLIND LINDIRECTA 2, Cambiar RSRCNAME CMNxx	Ha de tener el nombre del recurso 2838 anotado anteriormente. Si alguna de las lineas esta apuntando a un dispositivo que sea 268C no arrancará.			
WRKLIND EDITRANLIN 2, Cambiar RSRCNAME CMNxx NETADR XXXXXXXX <-NRI	Ha de tener el nombre del recurso 2745 anotado anteriormente.			
GO TCPADM 1. Configurar TCP/IP 1. Trabajar con interfaces TCP/IP Borrar todas las entradas. 2. Trabajar con rutas TCP/IP Borrar todas las entradas. 1. Trabajar con interfaces TCP/IP 1. Añadir + Intro INTNETADR > '10.250.6.XX' LIND > LINDIRECTA SUBNETMASK > '255.255.255.0' 2. Trabajar con rutas TCP/IP Destino Máscara Salto Opc Ruta Subred Siguiente				

1 *DFTROUTE *NONE 10.250.6.253				
GO TCPADM 1. Configurar TCP/IP 10. Trabajar con entradas de tabla de sistemas principales TCP/IP Configurar las direcciones IP de los sistemas.	Dirección Nombre Internet Sistema Principal			

Acción	Observaciones	Hora	T.Total	Fin Ok
Retener subsistema Q1ABRMNET				
Desactivar controladores de otras máquinas. WRKDEVD B44* (etc.)				
Restaurar las bibliotecas omitidas de BRMS en el siguiente orden RSTLIB SAVLIB(Q1ABRMSF Q1ABRMSF01 QUSRBRM QBRM) DEV(DEVICE)				
RSTAUT	RSTAUT debe hacerse también después de restaurar las bibliotecas de producción.			
En este punto habría que reaplicar PTFs que se hubieran aplicado después del salvado del sistema.				
Devolver los valores del sistema cambiados a sus valores originales.	QALWOBJRST = *ALWPTF QJOBMSGQFL = *WRAP QJOBMSGQMX = 64 QPFRADJ = 0 QVFYOBJRST = 3			
Retener los trabajos que sean susceptibles de arrancarse por el scheduler. WRKJOBSCDE				
DSPJOBLOG * *PRINT y comprobar que no hay errores de restaurado.				
WRKDEVD TAP* Desactivar dispositivos TAP*				
WRKHDWRSC *STG	Buscar recursos físicos para TAPMLB y TAP0*			
Antes de hacer IPL se han de cambiar los parámetros de los dispositivos de cinta y biblioteca de cintas para que se inicie sólo el TAPMLB05 WRKDEVD TAP0X 2, Cambiar --> En línea en IPL = *NO				

Poner nombre de recurso. WRKDEVD TAPMLB05 2, Cambiar --> En línea en IPL = *YES Cambiar nombre de recurso.				
Activar TAPMLB y comprobar que todo OK.				
Hacer IPL -Poner el panel en NORMAL PWRDWNSYS OPTION(*IMMED) RESTART(*YES *FULL) IPLSRC(B)				
Revisar estado de programas bajo licencia GO LICPGM Opc. 10	El estado debe ser *COMPATIBLE.			
Liberar los trabajos del scheduler que se han retenido anteriormente.	Sólo los absolutamente necesarios.			

Acción	Observaciones	Hora	T.Total	Fin Ok
Restaurado de Datos - Del salvado diario -				
Introducir cartucho save diario				
A partir de aquí se van a restaurar las bibliotecas de producción desde el salvado diario.	Importante.- Antes de comenzar con el restaurado asegurarse de que existen todas las listas de autorizaciones			
Restaurar desde el cartucho del salvado diario el fichero QUSRBRM RSTLIB SAVLIB(QUSRBRM) DEV(TAPMLB05) VOL('XXXXXX') MBROPT(*ALL) ALWOBJDIF(*ALL)				
Borrar grupos de red de BRMS GO BRMS 11 - 1 – 4	Para evitar que se comuniquen entre los sistemas.			
Comprobar políticas del sistema y grupos de control.				
A partir de aquí se puede usar BRMS				
Restaurar ZIPAVF con diferencia de objetos *ALL y *LEAVE	CRIPTO/CLAVESAVF			
Restaurar ZIPPPDAT con diferencia de objetos *ALL y *LEAVE	CRIPTO/CLAVESPP			
PKUNZIP ARCHIVE('ZIPAVF/SAVFAVF') TYPE(*EXTRACT) EXDIR('bib temporal/SAVFAVF') DROPPATH(*ALL) PASSWORD(CLAVE) OVERWRITE(*YES)				
RSTOBJ OBJ(*ALL) SAVLIB(AVF) DEV(*SAVF) SAVF(bib temporal/SAVFAVF) RSTLIB(AVF) ¡¡diferencias de objetos *ALL!!				
PKUNZIP ARCHIVE('ZIPPPDAT/SAVFPPDAT') TYPE(*EXTRACT) EXDIR('bib temporal/SAVFPPDAT') DROPPATH(*ALL) PASSWORD(CLAVE) OVERWRITE(*YES)				
RSTOBJ OBJ(*ALL) SAVLIB(PPDAT) DEV(*SAVF) SAVF(bib temporal/SAVFPPDAT) RSTLIB(PPDAT) ¡¡diferencias de objetos *ALL!!				
Desde BRMS restaurar	Comprobar logs.			

bibliotecas de salvado diario, poniendo permitir diferencias de objetos = *ALL y biblioteca destino = *SAVLIB				
Los ficheros encriptados en AVF son: SEFMASEG, SEFMSEPR, SEFMPOLI, SEFMPERC , SEFMBERE, SEFMEXTA, SEFMCUSB, SEFMCUSA , SEFMRCMD, SEFMPAGO, SEFMECON ,SEFMBERR , SEGMEXTA, SEGMCUSB, SEGMCUSA, SEFHRCMD, SEFMSINI, SEFWCINREA, SEFMCPRRE, SEFMDARE, SEFMOBTA ,SEFMTARI,SEGMOBTA				
Los ficheros encriptados en PPDAT son: FMPERS FMPARL FMPARG FMPERF FMPARC FMBENE FMEXPE				
Comprobar que los journals tienen enganchados los ficheros.				
Crear biblioteca GESTDOC con lista de autorizaciones SPOOLSAV				
Crear biblioteca BCKPEN y BCKSEG				
Restaurar bibliotecas CONTINPEN y CONTINSEG y copiar los ficheros a BCKPEN Y BCKSEG				

Acción	Observaciones	Hora	T.Total	Fin Ok
Configuración de aplicaciones				
RSF				
Poner clave de contingencias. RSF/CHGRSFAUT AUTH(XXXXXXXX) EXPDAT(AAAAMMDD) Configurar conexiones a servidores de RSF ADDLIBLE RSF ADDLIBLE RSFTOOLS WRKRSFSRV Aparecerá la lista de servidores. Opción 2 + Intro + Intro para cambiar la dirección IP en cada uno de ellos.				

Acción	Observaciones	Hora	T.Total	Fin Ok
Editran				
Cambiar datos (IP y NRI) del entorno local. EDITRANP 3, 1, M				
Cambiar NRI e IP en sesiones de pruebas. IGA 3, 4, M -> PRBCTG				
Antes de activar EDITRAN comprobar estado de la línea, controlador y dispositivo. EDITRANLIN ACTIVO EDITRNET ACTIVADO EDITRUSR DESACTIVADO				
CFT AS400				
Machacar el fichero WINNT/System32/Drivers/Etc/HOSTS con la copia. Machacar miembros CFTPARM1 y CFTPART1 del fichero CFTPROD1/UTIN con los miembros CFTPARMCTG y CFTPARTCTG	Hacer un envío entre redes para probar que funciona correctamente.			
CFT NT				
Machacar el fichero CFT/Sample/PARMTCP.SMP con PARMTCP.CTG y rearrancar CFT				
Pruebas de Usuarios				
Autorizaciones sobre el dispositivo DISP01S1 para que no fallen las pruebas de contabilidad.				

6.2.1. RSTAUT

El mandato Restaurar Autorización (RSTAUT) restaura las autorizaciones privadas a perfiles de usuario. Este mandato restaura la misma autorización sobre objeto, a objetos especificados en el perfil de usuario, que tenía cada perfil de usuario cuando se salvaron todos los perfiles mediante el mandato Salvar Sistema (SAVSYS) o el mandato Salvar Datos de Seguridad (SAVSECDTA).

Esto permite que permanezcan las autorizaciones existentes, otorgadas tras la operación de salvar. La autorización no puede restaurarse a los perfiles de usuario hasta que los perfiles se restauren en primer lugar en el sistema mediante el mandato Restaurar Perfil de Usuario (RSTUSRPRF) y todos los objetos (para los que se da autorización) se restauren en las mismas bibliotecas de donde se salvaron.

Los objetos pueden restaurarse mediante los mandatos Restaurar Biblioteca (RSTLIB) o Restaurar Objeto (RSTOBJ). Los documentos y carpetas pueden restaurarse utilizando el mandato Restaurar Objeto en Biblioteca de Documentos (RSTDLO).

Los objetos de configuración de dispositivo pueden restaurarse utilizando el mandato Restaurar Configuración (RSTCFG) o el mandato Restaurar Objetos en Directorios (RST).

Si se restaura todo el sistema, debe seguirse el orden siguiente. La utilización del mandato RSTAUT debe ser el último paso de la secuencia:

1. Restaure el sistema operativo. Es un método alternativo a cargar el programa. Esta acción restaura la biblioteca QSYS y garantiza que se encontrarán los perfiles de usuario proporcionados por IBM.
2. Restaure todos los perfiles de usuario salvados en el sistema (*ALL es el valor por omisión del parámetro USRPRF) utilizando el mandato RSTUSRPRF.

3. Restaure en el sistema todos los objetos de configuración y gestión de recursos del sistema (SRM) mediante el mandato RSTCFG.

4. Restaure todas las bibliotecas de usuario utilizando el mandato RSTLIB.

5. Restaure todos los objetos de biblioteca de documentos en el sistema con el mandato RSTDLO.

6. Restaure todos los objetos en los directorios con el mandato RST.

7. Restaure la autorización sobre objetos a los perfiles de usuario con el mandato RSTAUT.

Nota: Los pasos 2 a 7 se pueden efectuar más de una vez. Por ejemplo, después de restaurar los perfiles de usuario (paso 2), el usuario puede restaurar solamente las bibliotecas de aplicación muy importantes (paso 3) y, a continuación, restaurar la autorización sobre objetos (paso 7). Con ello se obtiene un sistema que funciona pero que sólo puede utilizar las bibliotecas muy importantes. Más tarde pueden restaurarse los restantes perfiles de usuario, seguidos de las operaciones para restaurar las bibliotecas y la autorización sobre objetos.

Si las autorizaciones de un perfil de usuario se restauran mediante el mandato RSTAUT, el perfil de usuario debe restaurarse de nuevo para poder restaurar otras autorizaciones del mismo.

Si se restaura un perfil de usuario, debe seguirse el orden siguiente. La utilización del mandato RSTAUT debe ser el último paso.

- Restaure el perfil de usuario especificado en el sistema utilizando el mandato RSTUSRPRF.
- Restaure todos los objetos SRM y de configuración de dispositivos en el sistema con el mandato RSTCFG.

- Restaure las bibliotecas de usuario especificadas en el sistema con el mandato RSTLIB o RSTOBJ. Si el perfil de usuario se restaura porque el perfil existente en el sistema está dañado, las bibliotecas necesarias ya se hallan en el sistema, y no es preciso restaurarlas.
- Restaure todos los objetos de biblioteca de documentos en el sistema con el mandato RSTDLO.
- Restaure todos los objetos en los directorios con el mandato RST.
- Restaure la autorización sobre objetos del perfil de usuario con el mandato RSTAUT. El perfil especificado puede haberse restaurado con el mandato RSTUSRPRF.

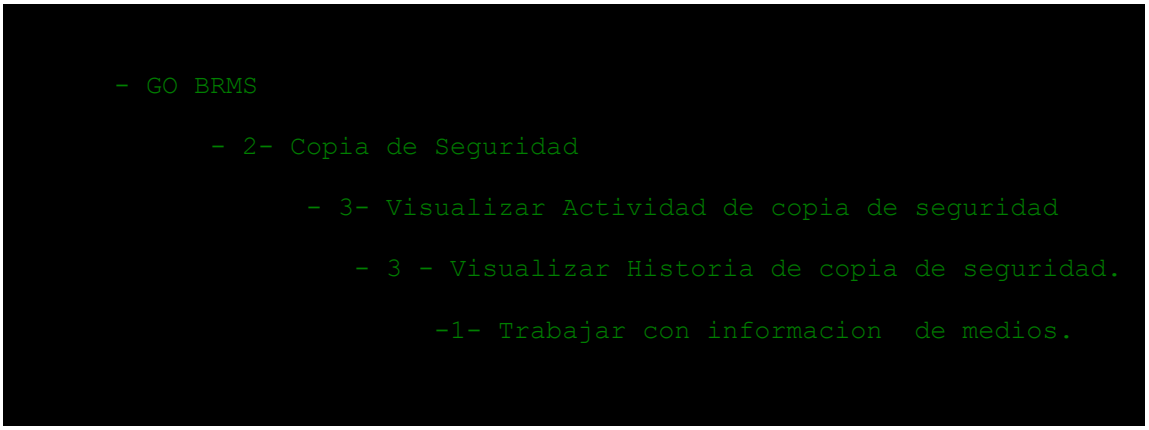
6.2.2. Mensajes de error para RSTAUT

Mensajes *ESCAPE

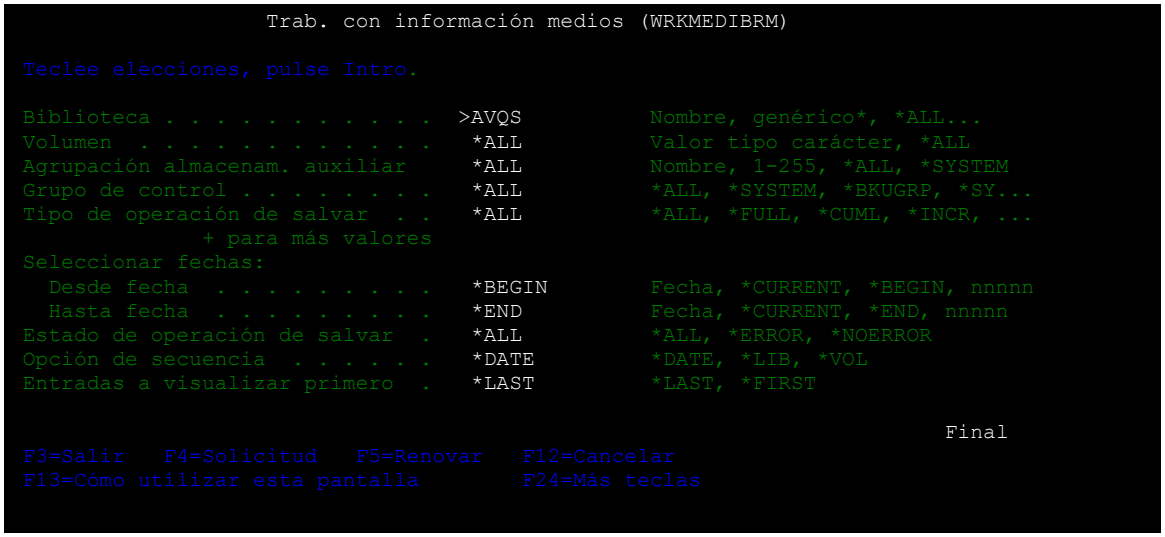
- CPF2206 El usuario necesita autorización para efectuar la función solicitada en el objeto.
- CPF222E Se necesita la autorización especial &1.
- CPF3776 No se han restaurado todas las autorizaciones de todos los perfiles de usuario.
- CPF3785 No han finalizado todos los subsistemas.
- CPF3855 RSTAUT no está permitido en este momento.
- CPF386D El trabajo de prearranque ha sufrido una anomalía.
- CPF9814 No se ha encontrado el dispositivo &1.
- CPF9833 Se ha especificado *CURASPGRP o *ASPGRPPRI y la hebra no tiene grupo de ASP.
- CPFB8ED La descripción de dispositivo &1 no es correcta para la operación.

6.3. Procedimiento para la restauración de datos mediante BRMS (procedimiento de operación)

Para buscar una libreria o un objeto en concreto en BRMS tendremos que seguir los siguientes pasos:



Utilizando el menú con las opciones arriba indicadas llegaremos a la pantalla donde solo tendremos que especificar el nombre de objeto, biblioteca, numero de volumen e incluso darle un rango de fechas dentro del cual queremos buscar. En el ejemplo vamos a buscar la biblioteca AVQS. Como se muestra en la pantalla de abajo solo hay que poner el nombre de la biblioteca para buscar en todos los cartuchos en que se encuentra.



Después nos aparecerá los cartuchos que contienen esa biblioteca.

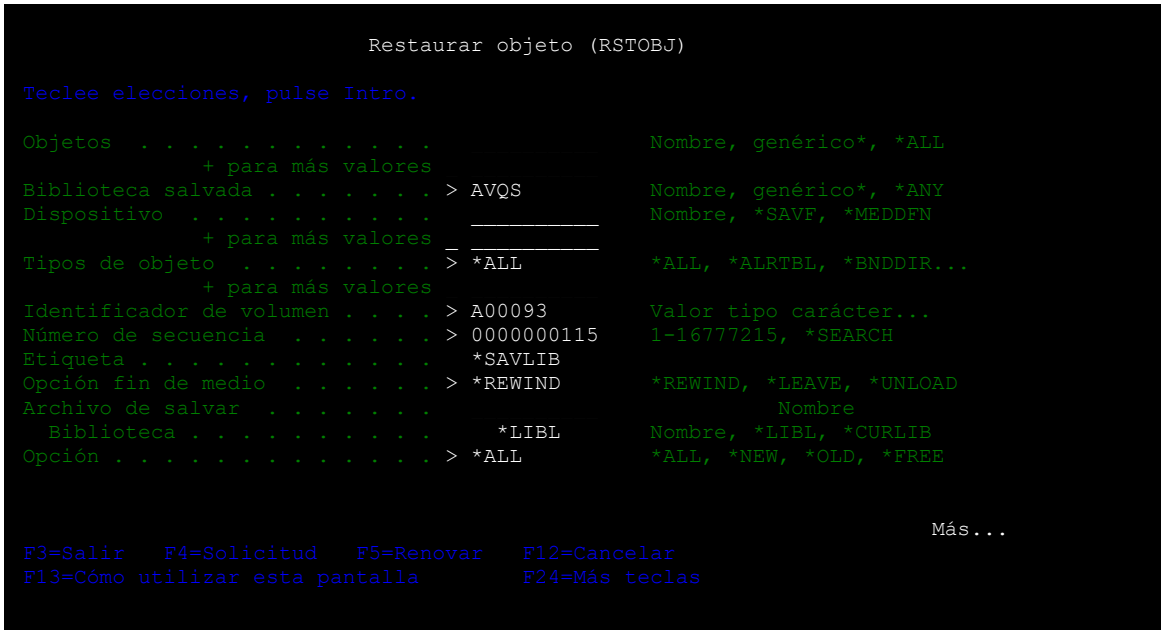
En esta pantalla solo tendremos que elegir según la fecha el que mas nos interese restaurar.

```
                    Trabajar con información de medios

 Situar en fecha  . . . . .

 Teclee opciones, pulse Intro.
   2=Cambiar  4=Eliminar  5=Visualizar  6=Trabajar con medios  7=Restaurar
   9=Trabajar con objetos salvados

    Elemento                          Tipo   N° serie   Secuencia  Fecha de
Opc salvado         Fecha     Hora    salvar volumen    de archivo caducidad
    AVQS           18/06/06  0:14:05 *FULL  000422          118   17/06/11
    AVQS           23/09/06 11:20:42 *FULL  000431          112   24/10/11
_   AVQS           16/12/06 11:58:01 *FULL  000483          112   15/12/11
_   AVQS           18/03/07  5:55:17 *FULL  000508          111   16/03/12
    AVQS           22/04/07  6:51:16 *FULL  000208          114   *VER EXP
    AVQS           19/05/07 12:43:41 *FULL  000434          115   *VER EXP
    AVQS           22/06/07 17:36:18 *FULL  000267          113   20/06/12
_   AVQS           13/07/07 18:13:28 *FULL  000340           79   *VER 003
_   AVQS           25/08/07 12:02:12 *FULL  A00085          116   *VER 003
    AVQS           16/09/07  6:42:38 *FULL  A00093          115   *VER 003
                                                                      Final

 F3=Salir   F5=Renovar
```

Después, si nos interesa un objeto en concreto volvemos a pulsar la opción 7 y le podremos especificar los objetos que queremos restaurar.

```
                  Seleccionar elementos de restauración

 Teclee opciones, pulse Intro. Pulse F16 para seleccionar todo.
   1=Seleccionar   4=Eliminar   5=Visualizar   7=Especificar objeto


     Elemento      Fecha    Hora    Tipo   N° serie Secuencia   Fecha   Objetos
Opc  salvado       salvar   salvar  salvar volumen  archivo   caducidad salvados
 7   AVQS        16/09/07  6:42:38  *FULL  A00093         115 *VER 003   6547









                                                                      Final
 F3=Salir F5=Renovar F9=Valores omisión restaurar F11=Ver ASP  F12=Cancelar
```

Especificamos los objetos a restaurar.



Y con un último INTRO procederemos a su restaurado.

7. Conclusión

El objetivo del proyecto era mejorar el estado de seguridad del sistema AS400 para llevarlo a un estadio de seguridad aceptable, mediante la ejecución de las recomendaciones detectadas.

Después de realizar las acciones técnicas necesarias se puede determinar que el estado actual del sistema es el esperado, no obstante es necesaria ejecutar de nuevo el análisis para poder evaluar los puntos que se han mejorado y poder establecer planes de acción para el mantenimiento correcto de la seguridad del sistema AS400.

Las áreas sobre las que se ha actuado son las siguientes:

- **Seguridad general**

Se ha evaluado la idoneidad del cambio en los valores del sistema para poder ejecutar los cambios en la seguridad general de forma correcta sin poner en peligro las operaciones del sistema. La mejora de la seguridad general aplica directamente a todo el sistema, subiendo a nivel de seguridad 40 que mejora la seguridad de la integridad del sistema.

- **Análisis de usuarios y seguridad de recursos**

Se ha realizado una aplicación para la gestión de usuarios y se ha adecuado el sistema al uso de este, limitando las capacidades de los usuarios y no excediéndose en los permisos que debían poseer. Se ha jerarquizado adecuadamente el sistema en los grupos establecidos y se han realizado un estudio minucioso de la seguridad de recursos.

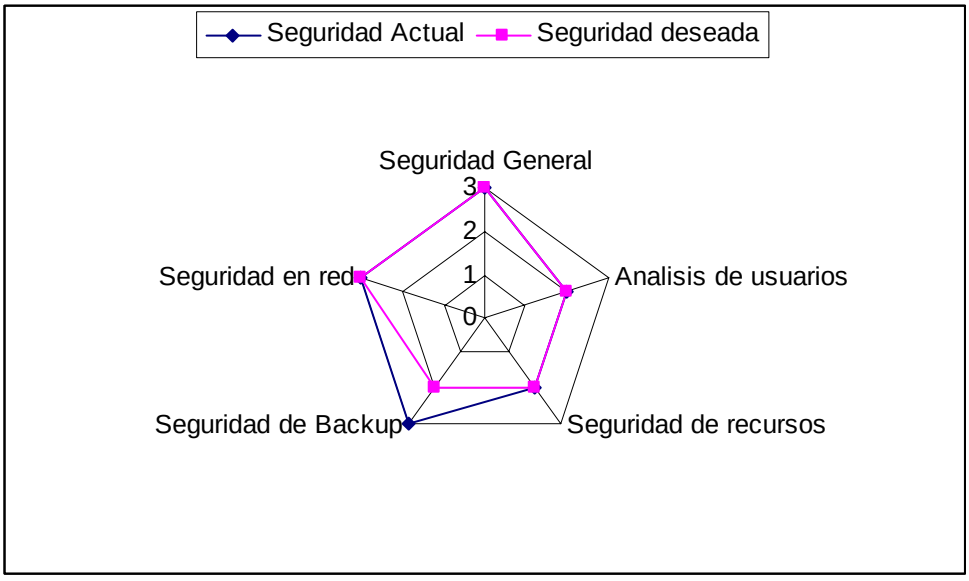
- **Seguridad en copias de seguridad.**

Se ha mejorado los procedimientos, dotando de seguridad y rapidez a la hora de recuperar el sistema.

- **Seguridad en red.**

Se ha mejorado la seguridad de la información que viaje en EDITRAN, garantizando la confidencialidad al aplicarle encriptación de los datos, además se ha puesto control a los accesos de los usuarios a la información mediante ODBC y otros medios no controlados.

Se puede concluir que el estado actual frente al estado deseado que se puede observar al inicio de este documento ahora es el mismo, consiguiéndose el objetivo propuesto, mejorando incluso la seguridad de backup por encima de la deseada.



Finalmente se puede afirmar que la calidad del sistema de seguridad es Parcialmente Satisfactoria si bien existen factores como la generación de políticas, la creación de la figura de Responsable de Seguridad, procedimientos de operación,… y otros puntos que escapan a la implantación de medidas técnicas que deben existir para poder garantizar el mantenimiento de este nivel de seguridad adquirido.

8. Bibliografía

1.1. Libros

[1] Carmel, Shalom. "*Hacking iSeries".* Ed. BookSurge Publishing. Febrero 2006.

[2] Dimmick, Roger; Hoskins, Jim. "*Exploring IBM AS/400 computers".* Ed. Gulf Breeze, FL : Maximum Press. 1997.

[3] Fottral, Jerry. "*Mastering the AS/400"*. Ed. 29th Street Press. Junio 2000.

[4] Gapen, Patrice; Stoughton, Catherine. "*Using the AS/400".* Ed. Danvers, Mass.: Boyd & Fraser. 1993.

[5] Gil Pechuán, Ignacio. "Arquitecturas hardware y telecomunicaciones". Ed. Universidad Politécnica de Valencia. 1998.

[6] Gil Pechuán, Ignacio. "*Implantación de sistemas y tecnologías de la información en las organizaciones". Ed. Universidad Politécnica de Valencia. 1998.*

[7] Guthrie, Gary; Madden, Wayne. "*Starter Kit for the IBM iSeries and AS/400".* Ed. 29th Street Press. Abril 2001.

[8] Hohly, Marge; Dawson, Mike. "*Understanding AS/400 System Operations".* Ed. MC Press. Junio 2000.

[9] Hoopes, Jim. *"AS/400 Client/server Crash Course".* Ed. Midrange Computing. Julio 1995.

[10] Hoskins, Jim. "*Building on Your OS/400 Investment: Moving Forward with IBM eServer iSeries in a On Demand World".* Ed. Maximum Press. Abril 2004.

[11] Hoskins, Jim; Dimmick Roger. "*Exploring IBM eserver iSeries".* Ed. Gulf Breeze, FL: Maximum Press. 2003.

[12] IBM. "*AS/400 Internet Security".* Ed.IBM. Junio 1997.

[13] IBM. "*AS/400 Internet Security Scenarios"*. Ed. IBM. Julio 2000.

[14] IBM. "*AS/400 TCP/IP Autoconfiguration".* Ed. IBM Redbooks. Mayo 1998.

[15] IBM. "*IBM System I Security Guide for IBM I5/Os Version 5 Release 4".* Ed. Vervante. Octubre 2006.

[16] IBM. *Managing OS/400 with Operations Navigator V5R1: Security.* Ed. IBM. Enero 2003.

[17] IBM. "*The System Administrator's Companion to AS/400 Avaliability and Recovery".* Ed. IBM. Agosto 1998.

[18] Lawrence, Jill T. *"AS/400 architecture and application".* Ed. Boston: QED Pub. Group. 1993.

[19] Lester, K. "*AS/400 Security, Audit and Control, First Edition"*. Ed. Elsevier Science. Febrero 1993.

[20] Madden, Wayne. "*Implementing AS/400 Security".* Ed. Duke University Press. Diciembre 1995.

[21] Marcelo Cocho, Julian Manuel. "*Riesgo y seguridad de los sistemas informáticos". Ed. Editorial UPV. 2003.*

[22] Musaji, Yusufali F. "*Autiding and security".* Ed. New York Wiley. 2001.

[23] Park, Joseph S. "*AS/400 security in a client/server environment".* Ed. New York Wiley cop.1995.

[24] Pence, Doug; Hawkins, Ron. "*iSeries and AS/400 APIs at Work".* Ed. MC Press. Abril 2001.

[25] Soltis, Frank G. "*Fortress Rochester : The Inside Story of the IBM iSeries".* Ed. 29th Street Press. Julio 2001.

[26] Stupca, Chuck. "*iSeries and AS/400 Work Management".* Ed. Mc Press. Enero 2002.

[27] Wenlock, Alison. "*The AS/400".* Ed. McGraw-Hill. 1996.

[28] Woodbury, Carol; Madden, Wayne. "*Implementing AS/400 Security, 4th Edition".* Ed. 29th Street Press. Octubre 2000.

1.2. Documentos en línea

[1] "*Application System/400. Cryptographic Support/400. Version 3*" http://publib.boulder.ibm.com/iseries/v5r1/ic2931/books/c4133420.pdf

[2] "*iSeries Security Reference*" http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi?CTY=US&FNC=SRX&PBL=SC41-5302-07

[3] "*Guia del usuario*" http://publib.boulder.ibm.com/tividd/td/as400/GC32-0279-01/es_ES/HTML/as40039.htm

[4] "*Information center*"
http://publib.boulder.ibm.com/iseries/v5r1/ic2931/index.htm

[5] "PowerTech. Proveedor de soluciones de seguridad para servidores IBM Midrange. Guias."
http://www.powertech.com/guides/Compliance/ComplianceGuide.htm#QRMTIPL.htm

[6] "*Comunidad de profesionales y usuarios de iSeries AS400 i5 server."*
www.recursos-as400.com