



Seguridad iSeries-AS/400 en un mundo en red

*Por John Earl, Jefe de Tecnología
Powertech Group, Inc.*

Versión del documento: 1.0

Fecha del documento: Abril 2003

Versión del producto: 1.0

1. Contenido

1. Contenido	2
2. El iSeries-AS/400 de IBM	3
3. Los problemas de seguridad del iSeries-AS/400	4
3.1 El Camino más corto en Seguridad	5
3.2 La llegada del PC crea inseguridad.....	6
3.3 Windows/95: El AS/400 escucha la alarma	7
3.4 Todos están conectados	7
3.5 TCP/IP e Internet.....	8
3.6 Soluciones para la seguridad del AS/400: Haciendo Reingeniería	9
3.7 Soluciones de Seguridad en AS/400: Acceso sólo a aplicaciones	10
3.8 Acceso por Exit Programs	11
4. Gestión de seguridad con iSeries Powerlock-Network Security	12
4.1 Tecnología PowerLock de gestión de exit-points	13
5. Seguridad y protección de datos con VISUAL Message Center.....	14
5.1 Tango/04 iSeries Security Agent	15
5.2 Gestión de sistemas con VISUAL Message Center	17
6. Servicios profesionales: Tango/04 y sus partners, a su servicio.....	18
6.1 Solución completa LOPD	18
6.2 Auditoría de seguridad y Certificación LOPD	18
6.3 Planes de contingencia y Alta Disponibilidad	18
6.4 Seguridad corporativa	19
7. LOPD, del reto a la oportunidad	20
8. Información adicional.....	22
8.1 Vínculos de interés.....	22
8.2 Acerca de Powertech Group, Inc.....	22
8.3 Acerca de Tango/04	23
8.4 Notas especiales y legales	24

2. El iSeries-AS/400 de IBM

El AS/400 – iSeries (en adelante AS/400) es tal vez el servidor de aplicaciones de negocios más vendido de IBM, ya que ha vendido más de 700.000 unidades desde su aparición en 1988. ¿Por qué? El AS/400 ofrece una escalabilidad sobresaliente, con modelos que van desde 2 a 3 usuarios hasta más de 10.000. El AS/400 es particularmente popular con entidades financieras, compañías de distribución y almacenamiento, al igual que con locales comerciales de venta al público.

Otro de sus atractivos es que todos los modelos de AS/400 usan el mismo sistema operativo. Esto ofrece a los desarrolladores de aplicaciones independientes una plataforma flexible con capacidad para ejecutar, en cualquier momento y en cualquier lugar, las aplicaciones ya escritas, creando un mercado extenso (desde pequeñas a grandes empresas) para sus aplicaciones de negocios. Estos desarrolladores de aplicaciones independientes (ISD por sus siglas en inglés) tienen escritas más de 35.000 aplicaciones que han ayudado a hacer del AS/400 uno de los servidores de negocios más populares.

Las compañías compran sistemas computarizados basándose en la habilidad de que estos se correspondan con sus necesidades de negocios, entonces si han un gran número de aplicaciones comerciales específicas en una plataforma particular, ésta se hace popular. Adicionalmente, el AS/400 puede soportar múltiples aplicaciones en un único servidor, facilitando a los clientes la integración de funciones de negocio similares en una sola máquina.

El AS/400 también tienen una excelente reputación por su fiabilidad, frecuentemente funciona durante meses o incluso años sin caídas imprevistas. Aunque suene gracioso, la fiabilidad del AS/400 limita la atención del mercado a este excelente sistema.

¿Por qué? Parece que prestamos más atención a los sistemas que necesitan alto mantenimiento y que a menudo vemos en periódicos y revistas. Incluso las compañías que tienen un AS/400 y lo usan para aplicaciones de negocio críticas parecen ignorar la máquina.

El AS/400 también tiene la reputación de ser uno de los servidores más seguros que se puede encontrar en el mercado hoy en día: una evidencia del poder del marketing de IBM.

Por razones que detallaré luego en este documento, esa reputación no es completamente precisa. En realidad, muchas organizaciones que creen que su información crítica está segura en su AS/400, se enfrentan a un riesgo tremendo.

3. Los problemas de seguridad del iSeries-AS/400

La arquitectura del AS/400 salió del “Proyecto de Sistemas Futuros” secreto lanzado por IBM en los años 70. El resultado de ese proyecto fue el anuncio del Sistema/38 de IBM en 1978. El sistema/38 ya era una aplicación orientada a objetos varios años antes que este tipo de aplicaciones fueran populares. Contenía una base de datos relacional integrada y seguridad a nivel de objetos. En esa época esto era una tecnología totalmente nueva.

La estructura orientada a objetos del sistema/38 era capaz de especificar la seguridad de forma muy selectiva. Perfiles de usuario individuales, perfiles grupales o todos los usuarios (*PUBLIC) podían tener autoridad para ejecutar programas, archivos u objetos individuales. El Sistema/38 era más notable aún: con él se podían definir autorizaciones a los programas, así como también a la información del sistema.

Claramente la seguridad del sistema/38 era poderosa, pero también asombrosa. Con cientos de usuarios y miles de objetos en un sistema, administrar la seguridad era una tarea muy difícil para los clientes del sistema/38. Los administradores del sistema buscaron el camino más corto y rápidamente adoptaron uno: “La Seguridad por Menú”.

3.1 El Camino más corto en Seguridad

Los administradores del sistema/38 rápidamente encontraron que ellos podía controlar el acceso de los usuarios usando una interfaz única a las aplicaciones y controlando las opciones disponibles. Se crearon menús por software para restringir usuarios a determinadas aplicaciones. Cuando entraban en el sistema, a los usuarios se les presentaba un menú propio hecho a medida. Si una opción de menú aparecía en la pantalla, era porque el usuario tenía autorización sobre los programas y archivos relacionados a esa opción de menú; de lo contrario, no había manera de que ese usuario pudiera acceder a los programas ni a los datos.

La simplicidad de la seguridad por menú fue la razón de su gran popularidad. Los administradores de sistema podían controlar el acceso al sistema de cientos de usuarios y evitaban tener que manejar la seguridad de miles de objetos. Para facilitar aun más las cosas los usuarios (o a veces el *PUBLIC) podían tener la autorización * CHANGE sobre los datos. En muchos lugares la seguridad de objetos era aun más simple: a los usuarios se les daba la autorización *ALL sobre los objetos.

Sin embargo, la Seguridad por Menú, asume que se accede al sistema solamente a través de una terminal, y que los menús de aplicaciones dan la seguridad necesaria a los terminales.

El Sistema/38 solo vendió 35.000 unidades en todo el mundo, pero su "hermano menor" el Sistema/36 fue mucho más popular, vendiendo más de 225.000 unidades desde su introducción en 1983.

Los administradores del sistema/36 usaban la seguridad por menú aun más que con el Sistema/38 porque su uso era muy sencillo. La razón principal era que el Sistema/36 no soportaba seguridad a nivel de objeto. En 1988 IBM anunció que el AS/400 era el reemplazo a las ya antiguas arquitecturas S/36 y S/38. Los clientes rápidamente adoptaron el nuevo AS/400 porque podían migrar sus aplicaciones ya hechas de forma fácil y rápida con la seguridad por menú y todo.

3.2 *La llegada del PC crea inseguridad*

El PC llegó al comienzo de la década de los 80 y se usó ampliamente en los negocios hacia el final de la década. El personal de sistemas y los usuarios finales adoptaron los PCs por su facilidad de uso y por la libertad de las políticas de uso corporativas. Desde el punto de vista de las empresas, los PCs se utilizaban inicialmente para emular las terminales. Es decir, los PCs estaban configurados con software y / o hardware para conectarse al AS/400 y emular las mismas terminales tontas que estaban reemplazando!

Los usuarios de PC pronto descubrieron las transferencias de datos desde y hacia el AS/400, así como los directorios compartidos, que permitían al PC acceder a los grandes discos virtuales del AS/400. El uso de impresoras compartidas se facilitó con las colas de impresión del AS/400 y algunos empezaron a usar el Remote Command.

Pero mientras el uso del PC crecía, la preocupación de los administradores del AS/400 iba en aumento. El PC era una seria amenaza de seguridad al AS/400, porque sus nuevas funciones no usaban la seguridad tradicional que se valía de menús de aplicaciones para determinar los derechos de acceso de los usuarios a los objetos.

Este problema fue discutido discretamente durante años por los técnicos del AS/400, pero no se hizo nada para corregir el problema, ya que la solución parecía muy costosa (rediseñar toda la arquitectura de seguridad del AS/400) o el riesgo se percibía como bajo.

Hubo 3 factores principales por los que los administradores del AS/400 creían que el riesgo era bajo:

- Los mandatos necesarios para aprovechar los huecos en la seguridad eran difíciles, eran mandados DOS desconocidos y únicos para el AS/400. Así que pensaron que era poco probable que un usuario final pudiera descubrirlos, y aun menos probable que un hacker pudiera reconocer su potencial destructivo.
- La mayoría de las instalaciones AS/400 eran stand-alone, o tenían muy pocas máquinas IBM concentradas en una red cerrada. El acceso a esta red (de entrada o salida) estaba normalmente contenido en un solo edificio.
- El sistema operativo del AS/400 (OS/400) y el protocolo de red (SNA) eran únicos para esta plataforma y se creía que no serían entendidos por los hackers entrenados en UNIX, que eran los más probables causantes de problemas.

3.3 *Windows/95: El AS/400 escucha la alarma*

Dos sucesos en 1995 cambiaron la forma en la que el personal de AS/400 percibía el riesgo: la salida al mercado de Windows 95 y la introducción del software de conectividad de PC Client Access. Con estas herramientas los usuarios de PC ahora tenían acceso directo a los recursos del AS/400, incluso con interfaz gráfica. Ya no era necesario aprender mandatos desconocidos DOS para acceder a los recursos del AS/400.

La interfaz gráfica del usuario (GUI) dio a los usuarios nuevas herramientas para que fácilmente pudieran hacer operaciones complejas, tales como transferencias de archivos con apretar un botón, acceso a registros vía ODBC con un clic del ratón, y borrado de objetos arrastrándolos a la papelera de reciclaje y todo gracias al Entorno de Red.

Todo este daño potencial era posible porque los usuarios finales tenían autorización *CHANGE o hasta *ALL en los objetos del AS/400, ya que casi toda la seguridad del AS/400 estaba basada en la creencia (actualmente se considera inapropiada) que la seguridad por menú podría mantener a los usuarios lejos de las cosas a las que se suponía no deberían tener acceso. Todas estas herramientas basadas en Windows permitían a los usuarios eludir la tradicional seguridad por menú y acceder a los recursos del AS/400 directamente, sin tener un acceso por terminal.

3.4 *Todos están conectados*

Para aumentar las preocupaciones de los administradores del AS/400, el uso de Internet empezó también a crecer significativamente durante el mismo período. La necesidad de realizar e-business cambió fundamentalmente las redes corporativas, haciéndolas más grandes, más heterogéneas y más abiertas.

Las compañías que alguna vez cerraron las redes internas, se encontraron conectadas a los proveedores, clientes, fuerza de venta móvil y otros. Algunos con seguridad, otros sin.

El peligro ahora venía potencialmente de cualquier usuario con acceso a la red, que ahora contaba con autorizaciones extraordinarias a los datos del AS/400 debido a la forma en que estaba establecida la seguridad tradicional del AS/400. Los administradores de sistema ahora tenían que conectar sus AS/400s a sistemas remotos que no estaban bajo su control. Estos sistemas podrían acceder a datos importantes del AS/400 eludiendo la tradicional seguridad por menú. Entonces los usuarios en redes remotas podrían potencialmente acceder a datos internos del AS/400, ¡sin que quedara ningún rastro de la transacción!

3.5 *TCP/IP e Internet*

IBM prefirió unirse antes que combatir con Internet y anunció que el AS/400 aceptaría e-business. Esto significaba pasar del protocolo propietario (SNA) al (TCP/IP), protocolo más estándar, más abierto. El uso de TCP/IP trajo aún más preocupaciones para los administradores de sistemas, estas preocupaciones incluían el FTP (protocolo de transferencia de archivos), el REXEC (capacidad de ejecutar mandatos remotamente) y el DDM (Administración distribuida de datos).

En su cambio de dirección hacia el e-business, IBM usó herramientas existentes en Internet provenientes del entorno UNIX, que incluían un File System (Sistema de Archivos) y el Command Shell Interpreter. Los desarrolladores UNIX fueron también invitados a trasladar sus aplicaciones al AS/400. La popularidad del AS/400 como un servidor para e-business ayudó al desarrollo de un grupo significativamente más grande de gente que tenía una profunda experiencia con el AS/400.

IBM ha tenido éxito en traer este servidor de medio alcance, anteriormente desconocido, al mercado como un servidor comercial potente y fiable para aplicaciones internas y externas. Mientras que los informáticos entienden mejor el AS/400, los hackers también lo hacen. Hasta hace algún tiempo el AS/400 estaba fuera de los intereses de los hackers, pero ahora ha ganado algunos seguidores. Se ha roto el velo del anonimato.

3.6 Soluciones para la seguridad del AS/400: Haciendo Reingeniería

Hoy en día hay tres corrientes principales de pensamiento referentes a la seguridad del AS/400: Re-ingeniería, Acceso solo a aplicaciones y Exit Programs.

Parece obvio que la mejor solución para asegurar el AS/400 es usar las herramientas disponibles en el sistema, haciendo re-ingeniería de las aplicaciones heredadas para utilizar la seguridad a nivel de objeto. Esta parece la solución más directa, pero es la más difícil.

¿Por qué? Un AS/400 típico más de 200 usuarios y 30.000 objetos separados. Asignar la autorización correcta a cada usuario y a cada objeto no solo tomaría mucho tiempo, si no que sería casi imposible por las complejas interrelaciones entre objetos. Una sola asignación de autorización errónea puede destruir una aplicación o hacer que los usuarios autorizados no puedan usar los datos a los que tienen acceso.

Las nuevas instalaciones de AS/400 interesadas en la seguridad, deberían usar la seguridad del sistema operativo a nivel de objetos. Pero las instalaciones existentes ven esta tarea costosa, larga y potencialmente peligrosa para las operaciones de negocios. El problema se vuelve aun más difícil para las instalaciones de AS/400 que usan software desarrollado por terceros.

Los proveedores de software de terceros, típicamente no estudian las necesidades de seguridad de sus propios paquetes y no pueden dar mucha ayuda sobre seguridad a sus clientes. La experiencia también muestra que cualquier cambio hecho por el cliente, es sobrescrito por el siguiente upgrade que haga el fabricante del software.

Por estas y otras razones, la solución más obvia (hacer re-ingeniería de aplicaciones) no ha sido mayormente adoptada por los técnicos de AS/400.

3.7 Soluciones de Seguridad en AS/400: Acceso sólo a aplicaciones

El Acceso sólo a Aplicaciones (AoA) es usado para restringir el acceso al AS/400 solo a aquellos usuarios que están inscritos en el sistema de menús de aplicaciones. Esto se logra cambiando el AS/400 de manera que un usuario (APPOWNER por ejemplo) es propietario de los datos y todos los otros usuarios son específicamente excluidos de tener acceso directo a los datos.

Un programa "gateway" es creado entonces para dar acceso a los datos (usualmente a través del sistema de seguridad por menús). Cuando se invoca el programa "gateway" este adopta la autorización del perfil APPOWNER, dándole así al usuario final la autorización para acceder a los datos. Esto tiene el beneficio de asegurar que solo se puede acceder a los datos a través del programa "gateway" y que la seguridad por menús es la que controla los accesos.

La desventaja del AoA es que a menudo es muy restrictivo para usuarios con legítima necesidad de transferir datos del AS/400 a aplicaciones en PC. Dado que el "gateway" es la única entrada autorizada a la aplicación, acceder a los datos del AS/400 desde cualquier conexión de red no está permitido.

Entonces, los administradores del AS/400 se ven forzados a dar a los usuarios acceso directo a archivos AS/400 específicos. Esto rápidamente se vuelve difícil de mantener, ya que distintos archivos son identificados para distintos usuarios y se asignan niveles de acceso específicos archivo por archivo.

Una vez que un usuario tiene acceso directo a un archivo, AoA no puede distinguir entre los distintos métodos usados para acceder al archivo. Si un usuario tiene la autorización necesaria para consultar datos mediante una aplicación Visual Basic, también tendrá los derechos necesarios para descargar el archivo completo usando otra herramienta (FTP por ejemplo) y sacar el contenido del archivo es secreto usando un diskette o el e-mail.

AoA también falla en ambientes de trabajos batch, donde la autorización adoptada es más difícil de propagar. El AS/400 no permite que la autorización de un usuario "viaje" a un trabajo batch sometido. Por lo tanto un administrado AS/400 tendrá que identificar todos los trabajos batch que existan en una aplicación y modificar aquellos programas para que también adopten la autorización APPOWNER.

Mientras esto pueda parecer factible para aplicaciones nuevas o para aquellas internamente desarrolladas que sean compactas y bien entendidas, es muy difícil por no decir imposible para aplicaciones desarrolladas por terceros o las desarrolladas internamente que no estén bien documentadas.

3.8 Acceso por Exit Programs

Los Exit Programs ofrecen un método para asegurar el acceso a datos específicamente vía la red. Los Exit Programs son programas simples hechos por el departamento de sistemas o por un proveedor externo que se definen para el AS/400 en puntos de salida de la red. Desde la salida del sistema operativo V4R4MO hay más e 50 puntos de salida de red que representan más de 300 tipos de transacción disponibles en el AS7400.

Si un punto de salida tiene un Exit Program registrado para sí, invocará al Exit Program por cada transacción al interior de la red. Los Exit Programs obligan algunas medidas de seguridad adicionales que son únicas para ese AS/400. Cuando un Exit Program es invocado, este recibe información acerca del tipo de transacción que se está solicitando, del perfil de usuario que está ejecutando la transacción y de los recursos del AS/400 a los que se está accediendo.

Los Exit Programs pueden imponer reglas de acceso basadas en usuario, ubicación del PC remoto, tipo de acceso, o en objeto. Entonces los administradores de AS/400 pueden regular el acceso a servicios específicos del AS/400 (FTP y ODBC por ejemplo) a usuarios específicos o a ubicaciones remotas específicas (usando direcciones TCP/IP o nombres SNA).

La dificultad de los Exit Programs es que el sistema operativo no ofrece ninguno. Deben ser escritos por el departamento de sistemas o comprados a un proveedor externo. Los Exit Programs pueden ser difíciles de escribir y probar ya que ellos requieren interfaces del sistema operativo de muy bajo nivel.

Las pruebas son complicadas porque los Exit Programs no se pueden aplicar en conexiones de prueba. Una vez instalados, estarán activos para todo el AS/400. Adicionalmente hay más de 300 tipos de transacciones distintas para motorizar, y nuevos de salida aparecen con cada nueva versión del sistema operativo.

Sin embargo, hay aplicaciones de seguridad con Exit Programs, como PowerLock, fabricadas por terceros que pueden bloquear accesos a usuarios individuales, a rango de direcciones TCP/IP como también a archivos de datos específicos. Una solución de este tipo tiene la ventaja de librar al departamento de sistemas de la carga que significa estar cubriendo todos los nuevos puntos de salida que van apareciendo con cada versión del sistema operativo, ya que de esto se encarga el proveedor.

4. Gestión de seguridad con iSeries Powerlock-Network Security

El AS/400 es la plataforma informática más segura del mercado gracias a que es la única que dispone de medidas de seguridad avanzadas integradas en el propio sistema operativo. Es el único sistema con derechos de seguridad a nivel de objeto para cada fichero, seguridad por menú y seguridad por aplicación.

Estas medidas eran perfectamente apropiadas para entornos AS/400 cuyos usuarios trabajaban a través de una de terminal "tonta" 5250 con aplicaciones alojadas en un *host* AS/400 "*stand-alone*", o bien en agrupaciones (*clusters*) AS/400 no conectadas en red.



Las redes locales (LAN), y posteriormente las de área extendida o remota, cambiaron los requerimientos de seguridad completamente, al proporcionar a los usuarios de PC acceso directo al AS/400 vía TCP/IP con aplicaciones como FTP.

Hoy en día los usuarios de PC rebasan totalmente la seguridad tradicional de menú y aplicación, y el AS/400 no provee una manera de detectar accesos a través de la red desde un PC. Las interfaces gráficas (GUIs) proveen herramientas muy poderosas que permiten a los usuarios de PC pueden cambiar datos o eliminarlos sin saberlo, y los comandos ocultos permiten también cambiar o eliminar datos en el AS/400. Un comando *update* de Excel, por ejemplo, puede sobrescribir ficheros DB2 del AS/400. El Entorno de Red de Windows (*Network Neighborhood*) hace que cualquier biblioteca AS/400, e incluso el sistema operativo OS/400, pueda ser eliminado desde un PC en red, sin dejar ningún rastro en el AS/400.

Las aplicaciones de terceros, por otra parte, trabajan con todos los derechos (por ejemplo, con el perfil de usuario QSECOFR) para tener más facilidad de uso y rendimiento mejorado. Sobrescriben la seguridad definida por el administrador cuando los *updates* son instalados, y proveen *exit Programs* para acceder datos a través de la red desde PCs conectados.

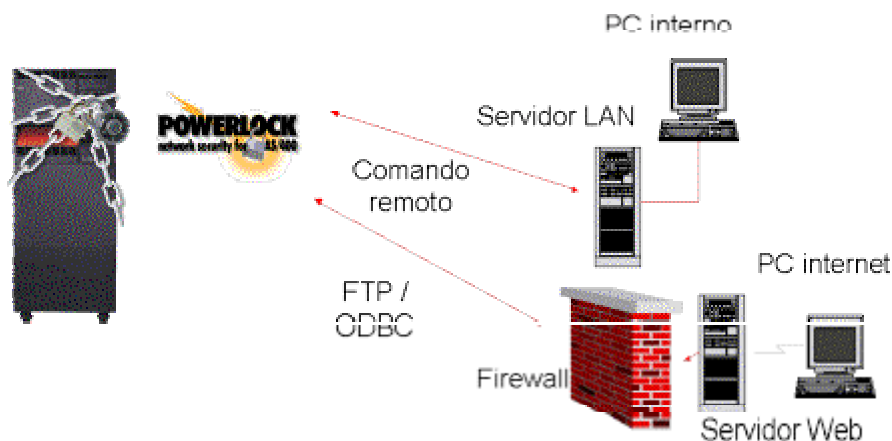
Con la aparición de Internet el AS/400 quedó expuesto además a la intervención de los *hackers*. Su conocimiento sobre AS/400 está creciendo y la tendencia es que la accesibilidad de los sistemas a través de la red también se incrementa.

PowerLock asegura el acceso de manera inteligente y efectiva sin impactar la productividad de los usuarios del sistema. Monitoriza *exit points* para limitar el acceso directo a datos del AS/400 a través de la red con servicios como FTP, Client Access, ODBC, etc., y audita intentos de acceso desde la red, tanto si son autorizados como si el sistema los deniega. Previene acceso a funciones restringidas y protege contra intrusiones accidentales o deliberadas sin afectar la funcionalidad necesaria para que el usuario de terminal puede realizar su trabajo cotidiano.

4.1 Tecnología PowerLock de gestión de exit-points

PowerLock usa tecnología de *exit points* para asegurar el acceso a datos en el AS/400. Los *exit programs*, escritos por usuarios o proveedores de aplicaciones, soportan funcionalidad cliente-servidor para proveer acceso a datos del AS/400. Pero también pueden ser utilizados para acceder a datos del AS/400 sin rastro o crear problemas de seguridad al integrarse con programas PC como FTP, Excel, Access y otras herramientas cliente-servidor.

PowerLock es una solución de gestión de seguridad inteligente que provee control selectivo por perfil de usuario, dirección IP o rango de direcciones IP. Provee alertas de seguridad a administradores de sistemas que pueden ser distribuidas inmediatamente mediante correo electrónico, buscapersonas, mensajes cortos SMS a teléfonos móviles, etc.



Estructura típica de funcionamiento de PowerLock.

PowerLock monitoriza más de 170 *exit points* para identificar intentos de acceso a datos AS/400 y permite al administrador de sistema seleccionar qué servidores y *exit points* van a ser vigilados, así como los tipos de transacción que van a ser monitorizadas.

PowerLock administra el acceso a servidores AS/400 por ODBC, FTP, DDA, DDM, y otros servicios que acceden vía *exit points*, impidiendo de forma selectiva que los usuarios entren en áreas a las cuales no están autorizados.

Con PowerLock, el Departamento de Informática tiene la capacidad de monitorizar problemas de seguridad, prevenir accesos de forma inteligente y controlar el acceso a datos AS/400 sensibles con un mínimo impacto en el rendimiento del sistema y sin que la productividad del usuario se vea afectada.

5. Seguridad y protección de datos con VISUAL Message Center

Para la mayoría de las pequeñas y medianas empresas, la mayoría de los riesgos en seguridad no provienen de hackers externos, sino de usuarios internos. Actuando con o sin intención, un usuario confuso o disgustado puede hacer un gran daño incluso al sistema más seguro.

El Agente de Seguridad de VISUAL Message Center ofrece la protección que las empresas necesitan. Constantemente monitoriza y audita el sistema buscando posibles problemas de seguridad y avisa a los operadores tan pronto detecta una incidencia.



VISUAL Message Center proporciona una solución única de monitorización, automatización y gestión centralizada de sistemas informáticos mixtos distribuidos. La consola gráfica de VISUAL Message Center, SmartConsole, centraliza la recolección y gestión de mensajes y eventos de sistemas tanto Windows como IBM eServer iSeries, permitiendo a los operadores gestionar estos sistemas de manera efectiva y con pocos recursos, reduciendo los costes operativos, mejorando el nivel de servicio del departamento informático, aumentando la disponibilidad de las aplicaciones, y permitiendo a los operadores concentrarse en proyectos estratégicos.

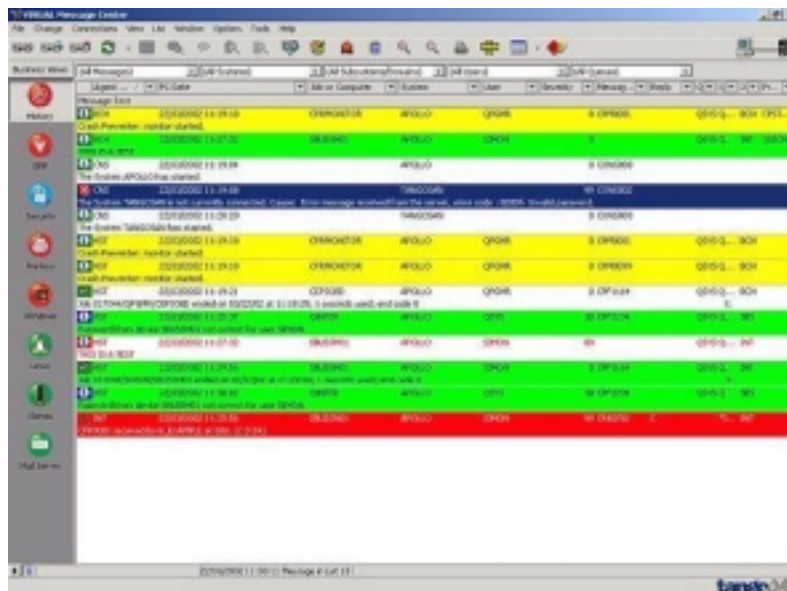


Fig. 2. Pantalla de monitorización SmartConsole con mensajes organizados en BusinessViews y codificados mediante colores

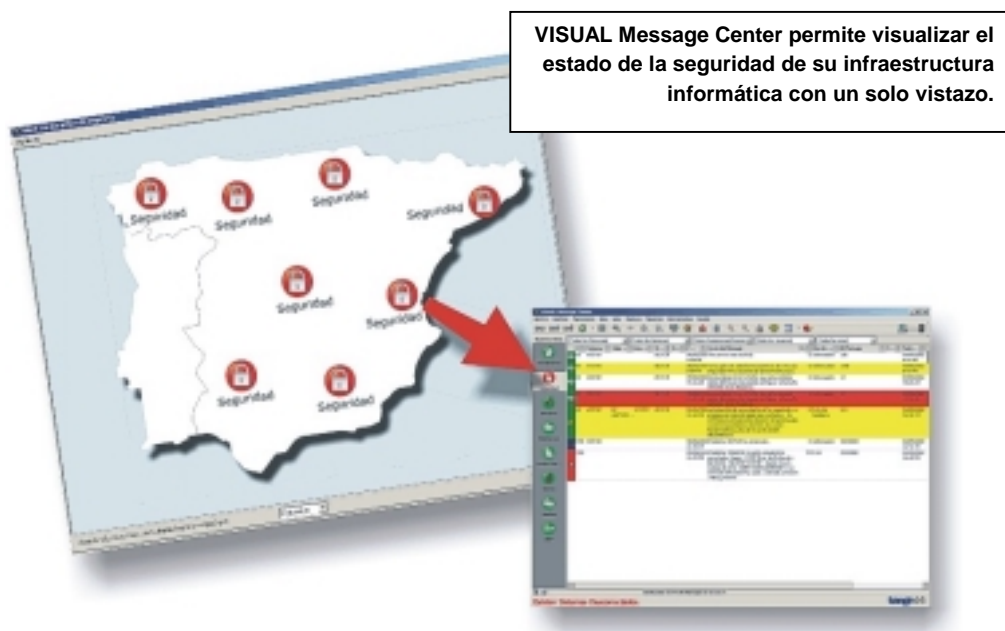
5.1 Tango/04 iSeries Security Agent

VISUAL Message Center proporciona una solución de gran alcance accesible para las pequeñas y medianas empresas, ofreciendo una gran y completa funcionalidad por una pequeña parte del coste y la complejidad que suponen los frameworks de gestión de sistemas.

iSeries Security Agent puede integrarse como parte de la estrategia de seguridad de la empresa, para realizar funciones de monitorización de seguridad en tiempo real y protección proactiva de la integridad de datos en sistemas iSeries y Windows.

Algunas de las funciones de iSeries Security Agent son:

- Consola central gráfica multi-sistema (SmartConsole), con flexibilidad para crear vistas (BusinessViews) específicas de eventos de seguridad.
- Detección en tiempo real de cambios en perfiles de usuario, objetos modificados o borrados, log-on incorrecto persistente, cambios en valores internos del sistema, uso de autorizaciones adoptadas, etc.
- Automatización de respuestas a condiciones críticas
- Automatización de alertas en tiempo real vía e-Mail, LAN y SMS.
- Integración con software de gestión de exit-points como PowerLock Network Security, firewalls de red, etc.



Con las alertas en tiempo real y las funciones de auditoría de VISUAL Message Center, la empresa puede gestionar la seguridad de sus sistemas pro-activamente, reaccionando de inmediato incluso a los más inesperados eventos.

Por ejemplo, podrá monitorizar posibles cambios no autorizados en el nivel de seguridad de su sistema (QSECURITY), actualmente ajustado a 50. Tan pronto como QSECURITY cambia, el Agente de Seguridad lo detecta, y puede restaurar automáticamente el nivel a su valor original, finalizando el trabajo que realizó la acción y desactivando el perfil de usuario utilizado.

Si lo que se desea es controlar el acceso a un fichero spool sensible para cumplir con el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que Contengan Datos de Carácter Personal, VISUAL Message Center trasciende los alcances de la auditoría y previene incidencias y violaciones de seguridad antes de que ocurran.

Un ejemplo de la vida real en una empresa podría constituirlo la existencia de un fichero denominado SALARIOS, que sólo puede ser accedido por el grupo de usuarios NOMINAS. El Agente de Seguridad puede monitorizar ese fichero, enviando una alerta si un usuario que no pertenece al grupo NOMINAS intenta acceder a él. El Oficial de Seguridad recibiría instantáneamente un aviso por e-Mail o SMS, con lo que podría tomar rápidamente una decisión.

Para cumplir los requerimientos de auditoría que establece el reglamento, iSeries Security Agent de VISUAL Message Center permitiría auditar los accesos a sistemas y ficheros con identificación individual de usuario y del momento en que se produce el acceso. La única función de auditoría no cubierta por VISUAL Message Center es la auditoría de acceso a nivel registro en ficheros que contienen datos especialmente protegidos, como podría ser el fichero SALARIOS.

iSeries Security Agent configura reglas de auditoría y gestiona eventos relevantes de seguridad usando poderosos filtros. Los eventos relevantes de seguridad recogidos pueden ser utilizados para auditar la seguridad del sistema e identificar posibles puntos débiles en cualquiera de las dos modalidades de auditoría que el producto ofrece:

Auditoría de Acciones:

Logs de eventos relevantes de seguridad de todo el sistema disponibles a nivel de sistema y/o nivel de usuario, por ejemplo, cambios o creación de perfiles de usuario, restauración de objetos, cambios de valores del sistema, acciones con ficheros de spool, etc.

Auditoría de Objetos:

Logs de eventos relevantes de seguridad relativos a objetos disponibles a nivel de sistema y/o nivel de usuario, con acciones automatizadas por cambios de objeto, o para todos los accesos a objetos, por ejemplo, borrado y copia de ficheros de bases de datos, cambios en las autorizaciones de los objetos, edición de ficheros, etc.

Los eventos críticos que pasen los filtros son enviados a la consola de VISUAL Message Center para que ésta instantáneamente envíe alertas o ejecute acciones automatizadas.

5.2 *Gestión de sistemas con VISUAL Message Center*

Basado en estándares de la industria y realizado en colaboración con IBM, el agente de seguridad y los agentes complementarios iSeries, Windows, Linux, UNIX y TCP/IP de VISUAL Message Center son la base de una solución realmente efectiva de seguridad en entornos iSeries-AS/400 que va todavía más allá, posibilitando la protección completa de toda la infraestructura corporativa. Incluye:

- Monitorización en tiempo real de sistemas multi-plataforma, locales y remotos.
- Detección inteligente de patrones de conducta sospechosos..
- Generación y escalamiento de alertas.
- Ejecución automática de acciones preventivas y correctivas en asignación de niveles de seguridad y acceso a recursos.
- Auditoría de acceso autorizado y denegado a recursos, objetos, programas, perfiles de usuario, archivos en spool, etc.
- Registro de incidencias.
- Definición de políticas de seguridad y protección automatizada (por ejemplo, restaurar el valor del nivel de seguridad de cada sistema si por error o malintencionadamente alguien intenta modificarlo).
- Personalización de reglas, alarmas, políticas y visualización gráfica corporativa a nivel de “tableros de mando” con el estado de procesos, usuarios, servidores, periféricos, etc (Enterprise Views).
- Extensible mediante estándares abiertos.

La funcionalidad de VISUAL Message Center trasciende los alcances de un proyecto de seguridad, añadiendo valor con funciones tales como gestión de rendimiento, monitorización centralizada de instalaciones remotas, soporte, alta disponibilidad y prevención de desastres. En reconocimiento a la vasta funcionalidad de VISUAL Message Center, Tango/04 es la única empresa europea entre las ocho que participan inicialmente con IBM en la Iniciativa de Informática Autónoma (antes proyecto eLiza), destinada a fomentar el desarrollo de soluciones de auto-configuración, auto-curación, auto-optimización y auto-gestión de sistemas informáticos.

6. Servicios profesionales: Tango/04 y sus partners, a su servicio

6.1 Solución completa LOPD

Además de proveer la tecnología y las herramientas que le permiten cumplir con la LOPD y asegurar su infraestructura informática, Tango/04 Computing Group cuenta con un equipo de consultores experimentados en la implantación de sistemas de seguridad en empresas de todos los sectores de actividad. Nuestro equipo profesional (y nuestros Partners certificados) están capacitados para prestar los servicios de planificación, integración, implementación y formación necesarios para el despliegue de una estrategia de seguridad y protección de datos en el contexto de la LOPD.

Por otra parte, Tango/04 ofrece a sus clientes otros servicios específicos relacionados con este tema que pueden ser prestados por solicitud en forma única o permanente:

6.2 Auditoría de seguridad y Certificación LOPD

Requerida cada dos años por la LOPD a las empresas que manejan datos protegidos con los niveles medio y alto de seguridad, la auditoría es un servicio mixto que puede incluir la instalación permanente de soluciones de software en los sistemas de una empresa o entidad, más la prestación periódica de servicios profesionales de auditoría basados en la información capturada por estas soluciones. Al contrario que la mayoría de empresas de auditoría, Tango/04 Computing Group puede realizar estas auditorías con un grado de detalle muy alto en entornos AS/400-iSeries, ayudándole a detectar posibles problemas, y recomendando soluciones técnicas prácticas, implementables en su mayoría rápidamente y sin esfuerzo.

6.3 Planes de contingencia y Alta Disponibilidad

Conjuntos de medidas y acciones específicas que las empresas deben emprender en caso de destrucción parcial o total de sus datos, inoperabilidad de sus instalaciones y recursos o incumplimiento de una normativa o nivel de servicio específico en materia de seguridad. Están dirigidos a recuperar la integridad de los datos y satisfacer las exigencias internas y externas.

6.4 Seguridad corporativa

A través de nuestra larga relación con IBM y nuestros Business Partners, contamos con especialistas al máximo nivel internacional, certificados por IBM, que pueden prestar asesoría profesional en proyectos corporativos de self-assessment de seguridad, paso a nivel de seguridad 40 ó 50, definición de arquitectura y políticas de seguridad corporativas, procedimientos de contingencia, prevención de desastres y gestión de riesgos.

7. LOPD, del reto a la oportunidad

Sea cual fuere el nivel de protección que su empresa o entidad deba dar a sus datos de acuerdo con la LOPD, muchas empresas españolas están aprovechando esta oportunidad para resolver definitivamente el problema de la Seguridad en su iSeries o AS/400.

Ello obedece a la profunda transformación registrada en forma reciente en la forma en que operan habitualmente los sistemas informáticos corporativos, entre los cuales destacan los siguientes:

- Los esquemas de seguridad “por menú” o por aplicación se han quedado anticuados.
- Hay numerosos puntos de acceso a OS/400 que no pasan por menús.
- Cliente/Servidor, NetServer, DDM, ODBC, FTP, B2B, Web, e-commerce, etc, o el simple acceso vía Internet abren muchas “puertas” que es necesario proteger.
- Los auditores internos e internos necesitan información.
- La empresa necesita proteger sus datos de filtraciones a la competencia, cambios producidos por errores voluntarios o involuntarios, etc.



Además de satisfacer las necesidades específicas de seguridad previstas por la LOPD y su Reglamento, la solución de seguridad Tango/04 ofrece a las empresas con sistemas iSeries la oportunidad de actualizar todas las dimensiones del entorno seguro de sus sistemas:

- Seguridad de Acceso a datos a nivel de punto de entrada.
- Seguridad, Control y Auditoría de datos a nivel de objeto, ficheros y spools.
- Seguridad, Control y Auditoría de datos a nivel de lectura y modificación de registros.
- Auto-protección por políticas de seguridad de accesos.
- Auto-protección por políticas de cambios de configuración de seguridad.
- Ampliable a detección de intrusiones y eventos (virus, etc.) de otras plataformas (Windows, UNIX, Linux, etc.) para proteger completamente la empresa.
- Cifrado de copias de seguridad y registros históricos de auditoría.

- Cifrado y compresión de datos que se envían remotamente.
- Cifrado y compresión de históricos de registro de auditoría.
- Gestión gráfica centralizada con indicación visual del estado de toda la infraestructura informática de su empresa.
- Notificación y Registro de incidencias según lo previsto en la LOPD.
- Reportes completos de Auditoría en tiempo real e histórico a diversos niveles de detalle.
- Auditoría, Servicios, Formación y Proyectos respaldados por los máximos expertos internacionales en la materia

Por todo lo anterior, estamos a su disposición para ampliar cualquier duda sobre la LOPD, la seguridad en general, o su proyecto en particular. Puede comunicarse con Tango/04 Computing Group al teléfono 93 274 00 51 con Carlos Suárez Martell.

8. Información adicional

8.1 *Vínculos de interés*

Gestión de sistemas:	http://www.tango04.es/soluciones/sistemas/index.php
Gestión de seguridad:	http://www.tango04.es/soluciones/sistemaseguridad/index.php
ISeries Security Agent:	http://www.tango04.es/productos/vmc/securityagent.php
Solución LOPD de Tango/04:	http://www.tango04.es/lopd/index.php
Agencia de Protección de Datos:	http://www.agenciaprotecciondatos.org
PowerLock Network Security:	http://www.powertechgroup.com/pt-solutions_plns.html
Artículos sobre el tema:	http://www.powertechgroup.com/pt-solutions_whitepapers.html
DataMirror LiveAudit:	http://www.datamirror.com/livebusiness/liveaudit/
Auditoría de seguridad:	http://www.datamirror.com/solutions/security/

8.2 *Acerca de Powertech Group, Inc.*

PowerLock es una empresa estadounidense desarrolladora de software de seguridad para control de accesos, detección de intrusiones y valoración de vulnerabilidades en servidores IBM iSeries-AS/400.

La familia de soluciones de seguridad PowerLock, desarrolladas por reconocidos expertos en seguridad iSeries, han obtenido numerosos premios internacionales y son actualmente utilizadas por empresas de todos los tamaños y sectores de actividad, incluida la propia IBM.

Fundada en 1996, PowerTech cuenta entre sus clientes con corporaciones como Lear Corporation, Shell Canada, Bank of America, HSBC, Horseshoe Gaming, Tommy Hilfiger, y Peregrine, quienes utilizan sus soluciones de software para proteger sus datos más críticos.

En España, PowerLock protege los activos digitales de empresas como Aseval, Santander Central Hispano, L'Oréal, Diagonoda, Alcampo, Mapfre, Binter Canarias, GesBM (Banco Spirito Santo), Ramos Sierra y Bodegas Torres, entre otros.

8.3 *Acerca de Tango/04*

Fundada en Barcelona en 1991, Tango/04 Computing Group es la principal empresa europea desarrolladora de soluciones de gestión integral de sistemas informáticos dirigidos a optimizar el rendimiento de negocios de las empresas, asegurar su salud operativa y reducir los costes de propiedad y operación de sus recursos.

Tango/04 asegura la salud operativa de todas las funciones corporativas para permitir a las empresas emprender con éxito estrategias de Integración de Aplicaciones Corporativas, Alta Disponibilidad, Inteligencia de Negocios, Seguridad y e-Business, entre otras. Aprovechando su liderazgo en tecnología IBM iSeries (AS/400), Tango/04 ayuda a más de 3.500 clientes en más de 60 países a asegurar los niveles de servicio que necesitan para trabajar en tiempo real y alcanzar sus objetivos de negocio, sobre cualquier plataforma informática.

El software de Tango/04 es utilizado por compañías de todos los tamaños, en todas las geografías y en todos los sectores de actividad. Algunos de nuestros clientes son Chase Manhattan, Cardinal Health, Coca Cola, Credit Suisse Asset Management, Johnson & Johnson, Nestlé, Nike, Telmex, Toys 'R' Us y Viking Direct.

Tango/04 ha obtenido año tras año un crecimiento de sus beneficios de más de un 50%. Una continua inversión en investigación y desarrollo asegura que las soluciones de Tango/04's seguirán evolucionando de acuerdo a las necesidades de los clientes.

Tango/04 es una empresa privada con sede central en Barcelona y oficinas propias en España, Francia, Suiza, Argentina, Chile, Estados Unidos y Perú. Nuestra red de Business Partners certificados comercializa nuestras soluciones en otros grandes mercados como Estados Unidos, Canadá, Alemania, Japón, Reino Unido, Italia, Rusia y México.

Tango/04 es IBM Advanced Business Partner y ha recibido el premio All Star Partner World for Developers consecutivamente los últimos cinco años. Es también la primera empresa europea que participa con IBM en la Iniciativa de Informática Autónoma (antes proyecto eLiza), destinada a fomentar el desarrollo de soluciones de auto-configuración, auto-curación, auto-optimización y auto-gestión de sistemas informáticos.

8.4 *Notas especiales y legales*

La información contenida en este documento fue creada utilizando equipamiento e instalaciones específicas, y su aplicación se limita a esas combinaciones especiales de productos y niveles de versiones de hardware y software. Cualquier referencia en este documento a productos, software o servicios de Tango/04 Computing Group, no implica que Tango/04 Computing Group planea introducir esos productos, software o servicios en cada uno de los países en los que Tango/04 Computing Group opera o está representada. Cualquier referencia a productos de software, hardware o servicios de Tango/04 Computing Group no está hecha con el propósito de expresar que solamente pueden utilizarse productos o servicios de Tango/04 Computing Group. Cualquier producto funcionalmente equivalente que no infrinja la propiedad intelectual o condiciones de licenciamiento específicas se podría utilizar en reemplazo de productos, software o servicios de Tango/04 Computing Group. Tango/04 Computing Group puede tener patentes o estar pendiente de obtención de patentes que cubren asuntos tratados en este documento. La entrega de este documento no le otorga ninguna licencia a esas patentes. La información contenida en este documento no ha sido sometida a ningún test formal por Tango/04 Computing Group y se distribuye TAL COMO ESTA. El uso de esta información o la implementación de cualquiera de las técnicas, productos, tecnologías, ideas o servicios explicitados o sugeridos por el presente documento es responsabilidad exclusiva del cliente, y el cliente debe ser quien evalúe y determine la aplicabilidad y consecuencias de integrar esas técnicas, productos, tecnologías, ideas o servicios en el entorno operativo del cliente. Si bien cada ítem puede haber sido revisado por Tango/04 Computing Group en cuanto a su exactitud en una situación específica, no existe ni se otorga ninguna garantía de que los mismos o similares resultados puedan ser obtenidos en otras situaciones o instalaciones. Los clientes que intenten adaptar esas técnicas en sus propias instalaciones lo hacen bajo su propia cuenta, responsabilidad y riesgo. Tango/04 Computing Group no será en ningún caso responsable directo o indirecto de cualquier daño o perjuicio causado por el uso de las técnicas explicitadas o sugeridas en este documento, incluso si se han efectuado notificaciones de la posibilidad de esos daños. Este documento puede contener errores técnicos y/o errores tipográficos. Cualquier referencia en esta publicación a entidades externas o a sitios web han sido provistas para su comodidad solamente, y en ningún caso implican una validación, garantía o respaldo a esas entidades o sitios.

Las marcas siguientes son propiedad de International Business Machines Corporation en los Estados Unidos y/o otros países: AS/400, AS/400e, iSeries, e (logo)@Server IBM © Operating System/400, OS/400. Microsoft, Windows, Windows NT, Windows XP y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o otros países. Java y todos los logotipos y marcas basadas en Java son propiedad de Sun Microsystems, Inc. en los Estados Unidos y otros países. UNIX es una marca registrada en los Estados Unidos y otros países y se licencia exclusivamente a través de The Open Group. Otros nombres de empresa, productos o servicios pueden ser marcas registradas de otras empresas.