PowerTech
SECURITY SCAN

05.05.16

Gracias por usar Security Scan de Powertech y por dar el primer paso para garantizar la seguridad de su IBMi (System i®, iSeries®, AS/400®). Usted encontrará a continuación un resumen de los resultados obtenidos con información detallada. Los resultados de este análisis le proveerán información de gran utilidad sobre qué está en riesgo en su sistema y cómo mejorar la seguridad.

Aprenda cómo mantener sus equipos a salvo haciendo uso de estas soluciones de Powertech:

- Authority Broker
- Command Security
- Compliance Monitor
- DataThread
- Interact
- Network Security
- Policy Minder
- PowerAdmin
- RSA Secure ID
- Password Self Help
- StandGuard Anti-Virus

Asegúrese de revisar la Guía en línea de Cumplimiento de Powertech, la cual provee información detallada de cada tema y recomendaciones sobre cómo configurar y auditar los sistemas para cumplir con regulaciones como HIPPA y PCI.

*Este reporte contiene enlaces a la Guía en línea de Cumplimiento de Powertech, la cual provee información detallada de cada tema y recomendaciones sobre cómo configurar y auditar los sistemas para cumplir con regulaciones como HIPPA y PCI.

INFORMACIÓN DEL SCAN

Nombre del Sistema: SAMPLE

Fecha del informe: 03/04/2015

Modelo: 42A

Tipo: 8286-EPXF

LPAR: 7

Pgroup: P20

Versión: V7R2M0

CCSID: 00037

RESUMEN

Riesgo por Violación de Seguridad

ALTO

La mayoría de los servidores IBMi (AS/400, iSeries) hoy en día están abiertos a vulnerabilidades únicas de la arquitectura IBMi y de las aplicaciones en el sistema.

¿Qué es COBIT?

Security Scan revisa vulnerabilidades de seguridad en seis importantes categorías y las asocia a su correspondiente control en COBIT.

COBIT es una estructura de control para las mejores prácticas de TI que muchas firmas usan como guía de cumplimiento para Sarbanes Ovley (SOX) y otras regulaciones.

Resultados de Security Scan

✗

1 Acceso a Datos

DS 5.3 - Gestión de Identidades

DS 5.5 - Prueba, vigilancia y monitoreo de la seguridad

✓

2 Autorización Pública

DS 5.4 - Gestión de Cuentas de Usuario

✗

3 Seguridad por Usuario

DS 5.3 - Gestión de Identidades

DS 5.4 - Gestión de Cuentas de Usuario

△

4 Seguridad del Sistema

DS 5.9 - Seguridad del Sistema

✗

5 Auditoría del Sistema

DS 5.5 - Prueba, vigilancia y monitoreo de la seguridad

△

6 Privilegios de Administración

AI 3.2 - Protección de los recursos de infraestructura

DS 5.3 - Gestión de Identidades

Herramientas de Software de Monitorización

El personal de Seguridad Informática necesita herramientas de software de calidad para monitorizar, detectar y bloquear violaciones de seguridad. Un número enorme de transacciones de negocio se realizan en los sistemas diariamente y cualquiera de ellas puede ser importante para la seguridad. Un usuario típico de IBMi genera entre 50 y 300 eventos de auditoría de seguridad por día.

Cantidad de IDs de usuario

68

Transacciones por día

3,400 - 20,400

YEl sistema tiene 68 IDs de usuario, lo que se traduce en 3,400 hasta 20,400 transacciones por día. En la medida en que los usuarios son cada vez más sofisticados, la cantidad de eventos de seguridad se incrementa, haciendo más difícil detectar las violaciones de seguridad.

1 ACCESO A REDES

Seguridad del Acceso a Redes

La seguridad del acceso de los usuarios a través de la red está en riesgo en este sistema. El IBMi se provee con una variedad de servicios de red que están configurados de fábrica y listos para comunicarse con otros equipos. Todos los sistemas IBMi deben contar con programas de salida (exit programs) en los servicios de red para monitorizar y controlar los accesos.

Objetivos relevantes de COBIT

COBITDS5.3 : Gestión de Credenciales

Asegure que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas (aplicaciones de negocio, operación del sistema, desarrollo y mantenimiento) sea unívocamente identificable.

COBITDS5.5 : Prueba, vigilancia y monitoreo de la seguridad

Pruebe y monitorice la implemetaciónde la seguridad de TI de forma proactiva. La seguridad de TI debe ser revisada periódicamente para asegurar que los estándares aprobados de la seguridad de la información de la compañía se cumplen. La registración y la monitorización permiten la detección temprana y la prevención permitiendo la generación a tiempo de reportes de actividad inusual o anormal que requiera ser revisada. Ver más en Guía de Cumplimiento de Powertech

Los servicios de red más visibles son

FTP

El servicio FTP permite subir datos desde una PC al sistema IBMi y bajar datos a cualquier PC. Cualquier usuario desde una PC puede ejecutar los comandos estándares de FTP como ls (list directories), cd (change directories), put(upload) y get (download).

¡Exposición!
- En SAMPLE, actividad FTP no está siendo monitorizado con programas de salida, ni tampoco hay reglas de control de acceso para prevenir la transferencia de datos vía FTP.

Bases de Datos

Las conexiones ODBC a bases de datos permiten manipular información en ficheros de bases de datos en los sistemas IBMi usando comandos standard de SQL como UPDATE, SELECT, DELETE. La mayoría de las PCs tiene drivers ODBC instalados que permiten a los usuarios acceder directamente a los sistemas IBMi. En muchos casos, es tan simple como seleccionar una opción de un menú en Excel.

¡Exposición!
- En SAMPLE, el servidor de base de datos no está siendo monitorizado con programas de salida, ni tampoco hay reglas de control de acceso para prevenir la manipulación de datos por parte de los usuarios vía conexiones ODBC.

Comando remoto

Cualquier usuario desde una PC con IBM Client Access puede ejecutar comandos remotos en un sistema IBMi al cual esté conectado. La limitación de acceso a línea de comandos en la configuracipón del perfil de usuario NO impide la ejecución remota de comandos.

¡Exposición!
- En SAMPLE, la actividad por comandos remotos no está siendo monitorizada con programas de salida, ni tampoco hay reglas de control de acceso para prevenir que los usuarios ejecuten comandos críticos desde una PC.

1 ACCESO A REDES

Programas de salida de IBMi registrados

Programas de salida faltantes

DDM

Distributed Data Management (DDM) es un protocolo de IBM que provee acceso remoto a ficheros de base de datos a usuarios y aplicaciones. El acceso vía DDM a este sistema es no asegurado.

Acceso a línea de comandos

0 62

59 DE 62

Hay 62 perfiles de usuario que tienen acceso a la línea de comandos, de los cuales 59 están habilitados.

Si un usuario tiene acceso a la línea de comandos (LMTCPB *NO or *PARTIAL), potencialmente puede ejecutar más de 2000 comandos que vienen disponibles en el sistema operativo. Algunos comandos son inocentes, como DSPJOB o DSPLIB. Sin embargo, otros como ENDJOB, ENDSBS o DLTJOB son peligrosos, si son utilizados en entornos no protegidos. Si un usuario tiene acceso a la línea de comandos, su poder es casi ilimitado. Se puede utilizar el atributo LMTCPB de los perfiles de usuario para limitar el acceso.

Servicios de red más visibles:

	Servicio de punto de salida (exit point)	Descripción	Programa de salida (exit program)	Importancia
1	*FILESRV	Remote File Server - Used when drives are mapped to IFS		ALTA
2	*TFRFCL	Client File Transfer Server		ALTA
3	*FTPSERVER	File Transfer Protocol (FTP) server on the System i		ALTA
4	*FTPREXEC	Remote command thru FTP		ALTA
5	*REXEC_SO	Remote Command Sign-on (log on)		ALTA
6	*SQL	ODBC & JDBC Sign on (log on)		ALTA
7	*NDB	ODBC & JDBC Native Database		ALTA
8	*RTVOBJINF	ODBC & JDBC Retrieve Object Info		ALTA
9	*SQLSRV 1	ODBC & JDBC Server		ALTA

1 ACCESO A REDES

	Servicio de punto de salida (exit point)	Descripción	Programa de salida (exit program)	Importancia
10	*SQLSRV 2	ODBC & JDBC Server	✖	ALTA
11	*RMTSRV	Remote Command Server	✖	ALTA
12	*DQSRV	Client Data Queue Server	✖	MEDIA
13	*TELNET	TCP/IP Terminal Emulation	✖	MEDIA
14	*FTPCLIENT	File Transfer Protocol (FTP) client on the System i	✖	MEDIA
15	*TFTP	Trivial FTP	✖	MEDIA
16	*DATAQSRV	Remote Data Queue Server	✖	MEDIA
17	*LMSRV	Client License Server	✖	BAJA
18	*MSGFCL	Client Message Server	✖	BAJA
19	*QNPSERVR	Virtual Print Server : (Entry)	✖	BAJA
20	*QNPSERVR	Virtual Print Server : (Spool File)	✖	BAJA
21	*RQSRV	Client Remote SQL Server	✖	BAJA
22	*FTPSIGNON 1	Allow/Prevent Anonymous FTP	✖	BAJA
23	*VPRT	Client Virtual Print Server	✖	BAJA
24	*CNTRLSRV	Client Access License Server: (License Mgt)	✖	BAJA
25	*CNTRLSRV	Client Access License Server: (Conversion Map)	✖	BAJA
26	*CNTRLSRV	Client Access License Server: (Client Mgt)	✖	BAJA
27	*SIGNON	OS/400 Signon Server	✖	BAJA

2 AUTORIZACIÓN PÚBLICA

Autorización Pública sobre bibliotecas

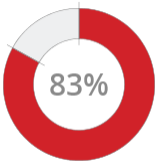
RIESGO BAJO

Los sistemas IBMi están provistos de un conjunto de permisos por omisión para las autorizaciones públicas (*PUBLIC)..

El acceso de *PUBLIC a las bibliotecas es una medición que muestra el nivel de acceso que tiene el usuario promedio sobre el sistema. Como lo establece el sistema operativo, *PUBLIC representa a cualquier usuario que puede logearse y que no tiene permisos explícitos.

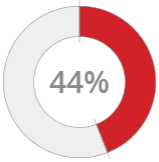
Para saber más sobre cómo monitorizar y auditar la configuración de permisos sobre bibliotecas lea Guía de Cumplimiento de Powertech

Permisos *PUBLIC



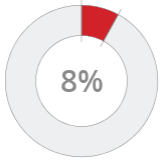
Todos los usuarios (*PUBLIC) que tienen permisos de lectura o modificación sobre las bibliotecas en el sistema.

*CHANGE



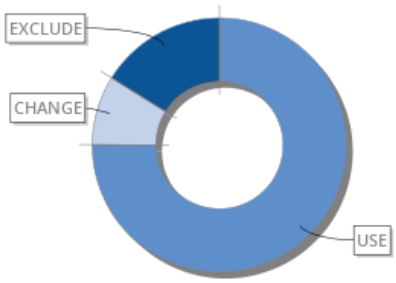
A *PUBLIC se le asigna "*CHANGE" sobre aquellos objetos que se creen nuevos en 30 bibliotecas.

Borrado de datos



Todos los usuarios pueden borrar datos o aplicaciones de más de 6 de las bibliotecas.

Permisos para *PUBLIC en bibliotecas



Autorización	Bibliotecas	Porcentaje
USE	51	75.0
CHANGE	6	8.8
ALL	0	0.0
AUTL	0	0.0
USER DEF	0	0.0
Read and oper	0	0.0
EXCLUDE	11	16.1

Cantidad total de bibliotecas en este sistema: 68

Aprenda más sobre cómo monitorizar y auditar la configuración de permisos sobre bibliotecas en Guía de Cumplimiento de Powertech

3 SEGURIDAD POR USUARIO

Seguridad por usuario y contraseñas

RIESGO ALTO

La seguridad por usuario y contraseñas es crítica porque es la forma más simple de poner en peligro un sistema. En este sistema los controles para usuarios y contraseñas se han revisado y se obtuvieron los siguientes resultados.

Recomendaciones de IBM sobre políticas de contraseñas

Los requerimientos de ISO 27002

Estas son las recomendaciones para las políticas de contraseñas basadas en las recomendaciones de IBM y del standard ISO27002 (conocida como 17799), que proveen una guía detallada para establecer políticas de contraseña robustas y gestión de cuentas de usuario. COBIT remarca la necesidad de una gestión efectiva de las cuentas de usuario.

COBIT DS5.3: Gestión de Identidades

Asegure que todos los usuarios (internos, externos y temporales) y su actividad en los sistemas (aplicaciones de negocio, operación del sistema, desarrollo y mantenimiento) sea unívocamente identificable.

COBIT DS5.4: Gestión de Cuentas de Usuario

Defina un conjunto de procedimientos para la gestión de cuentas de usuario, que especifiquen solicitud, uso, suspensión, modificación y eliminación de cuentas de usuario y privilegios de usuario. Incluya un procedimiento de aprobación por parte de los dueños los datos o los sistemas para garantizar el otorgamiento de privilegios.

La siguiente información muestra de manera resumida la seguridad por usuario y contraseñas:

Seguridad por Usuario

Las 2 áreas son de alto grado de preocupación:

Categoría	Recomendaciones	SAMPLE
Cantidad de IDs de usuario inactivos	0	✖3(3 Habilitado)
Cantidad de usuarios con intentos inválidos de conexión	Menos de 5	✔0
Cantidad máxima de intentos inválidos de conexión de un usuario	Menos de 3	✔0
Perfiles de usuario no seguros	0	✔0
Usuarios con contraseñas por defecto	0	✖7(6 Habilitado)

Configuración de Contraseñas

La tabla de configuración de contraseñas muestra que el conjunto de las reglas de contraseñas es débil en este sistema.

Configuración de Contraseñas	Estándar	SAMPLE
Expiración	90 Días	✖*NONE
Longitud mínima	6 Caracteres	✖4 Caracteres
¿Dígitos requeridos?	Si	✖No
Diferente a anterior	10 Contraseñas	✖0 Contraseñas
Bloquear Cambio de Contraseña	24 Horas	✖*NONE
Reglas de Contraseña	Por Política Corporativa	⚠*PWDSYSVAL

Aprenda más sobre Seguridad por usuario y contraseñas en Guía de Cumplimiento de Powertech

4 SEGURIDAD DEL SISTEMA

Seguridad del Sistema

El sistema operativo provee una serie de métodos para asegurar al sistema y las estaciones de trabajo conectadas a él. En esta sección se examinan los valores del sistema que protegen al sistema operativo y las estaciones de trabajo.

Objetivos relevantes de COBIT

COBIT DS5.9: Prevención, detección y corrección de software malicioso.

Establezca mediciones preventivas, de control y correctivas (especialmente parches de seguridad actualizados y control de virus) en toda la organización para proteger los sistemas de información y la tecnología de malware (por ejemplo, virus, worms, spyware, spam).

Aprenda más sobre Seguridad por usuario y contraseñas en Guía de Cumplimiento de Powertech

Valores del sistema que protegen el sistema operativo y las estaciones de trabajo:

Valor del Sistema	Comentarios	Valor	Calificación
QSECURITY	Su sistema está ejecutando a nivel 40 (QSECURITY), el valor mínimo recomendado por IBM.	40	BUENO
QALWOBJRST	No hay restricciones sobre el tipo de programas que se pueden cargar en este sistema. Un programador con conocimientos (incluyendo un proveedor o un contratista) podría cargar programas violando su seguridad sin ser detectado.	*ALL	DÉBIL
QVFYOBJRST	No se verifican las firmas de los programas al momento de su carga en el sistema. La fuente y la autenticidad de los programas del sistema operativo no pueden ser validados por este sistema.	1	DÉBIL
QUSEADPAUT	Cualquier usuario puede crear programas que adoptan autorización de otro usuario.	*NONE	DÉBIL
QDEVRCYACN	Los trabajos que experimentan un fallo de comunicación se finalizan automáticamente.	*DSCMSG	BUENO
QINACTITV	Los trabajos interactivos en este sistema no caducan por falta de uso.	*NONE	DÉBIL
QLMTDEVSSN	No hay límite en la cantidad de sesiones concurrentes que puede iniciar un usuario.	0	MODERADO
QLMTSECOFR	No existen restricciones referentes a en qué estaciones de trabajo puede conectarse el oficial de seguridad.	0	MODERADO
QMAXSIGN	Se le permite a los usuarios 5 intentos de conexión antes de tomar una acción.	5	MODERADO
QMAXSGNACN	Estación de trabajo	1	MODERADO

4 SEGURIDAD DEL SISTEMA

Anti-virus

La configuración apropiada de valores del sistema relacionados a funciones de save y restore ayuda a garantizar que no se instala software malicioso o inapropiado en el sistema.

Valor del Sistema	Comentarios	Valor	Calificación
QSCANFS	Stream files ubicados en los file systems root (/), QOpenSys y de usuario serán escaneados de amenazas de virus.	*ROOTOPNUD	BUENO
QSCANFSCTL	Todos los accesos serán escaneados, lo cual puede degradar la performance de las aplicaciones o del sistema.	*NONE	MODERADO

No hay control de virus cuando se abren ficheros.

No hay control de virus cuando se cierran ficheros.

5 AUDITORÍA DEL SISTEMA

Funcionalidades de la Auditoría del Sistema

RIESGO ALTO

Una importante funcionalidad del sistema operativo es registrar eventos importantes de seguridad en el registro de auditoría.

- La auditoría del sistema no está activada.
- El registro de auditoría (QAUDJRN) no existe en SAMPLE.

El valor del sistema de auditoría para objetos nuevos está establecido para no auditar a los objetos. (QCRTOBJAUD)

Registro de datos y herramientas de auditoría NO están en uso.

Registro de datos	Herramientas de auditoría
✗	✗

Auditoría de eventos de red: El sistema operativo proporciona múltiples puntos de salida que hacen posible la monitorización de la red en sus servicios más comunes como FTP, ODBC y DDM.

Usted puede revisar qué exit points están monitorizados en Acceso a Redes sección.

Valor de Auditoría	Descripción	Valor	Importancia
*AUTFAIL	Auditar fallos de autorización	✗	ALTA
*CREATE	Auditar la creación de objetos nuevos	✗	ALTA
*DELETE	Auditar el borrado de objetos	✗	ALTA
*PGMFAIL	Auditar los fallos de programas causados por violaciones de seguridad	✗	ALTA
*PTFOPR	Auditar operaciones PTF	✗	ALTA
*SAVRST	Auditar acciones de restauración de objetos sensitivos para la seguridad	✗	ALTA
*SECURITY	Auditar cambios de seguridad	✗	ALTA
*SERVICE	Auditar el uso de herramientas de servicio del sistema y de hardware	✗	ALTA
*JOBDTA	Auditar eventos de trabajos como inicio y fin	✗	MEDIA
*OBJMGT	Auditar cambios de gestión de objetos	✗	MEDIA
*PGMADP	Auditar el uso de programas que adoptan autorización	✗	MEDIA
*PTFOBJ	Auditar cambios de objetos de PTF	✗	MEDIA
*SYSMGT	Auditar cambios a ciertas áreas de gestión del sistema	✗	MEDIA

5 AUDITORÍA DEL SISTEMA

Valor de Auditoría	Descripción	Valor	Importancia
*NETCMN	Auditar eventos de firewall APPN	✖	BAJA
*NETSCK	Auditar tareas de sockets	✖	BAJA
*NETSECURE	Auditar conexiones seguras de red	✖	BAJA
*NETTELSVR	Auditar conexiones del servicio TELNET	✖	BAJA
*NETUDP	Auditar tráfico de UDP (User Datagram Protocol)	✖	BAJA
*OFCSRV	Auditar cambios de seguridad de Vision/400	✖	BAJA
*OPTICAL	Auditar el uso de dispositivos de almacenamiento óptico	✖	BAJA
*PRTDTA	Auditar funciones de impresión	✖	BAJA
*SPLFDTA	Auditar el uso de spooled files (reportes)	✖	BAJA

6 PRIVILEGIOS DE ADMINISTRACIÓN

Riesgo de Privilegios de Administración

RIESGO MEDIO

Los privilegios de administración se denominan permisos especiales. Estos permisos son muy poderosos y deben otorgarse solo a profesionales confiables y entrenados del área de TI. Aquellos usuarios que gocen de estos permisos deben ser auditados.

Quienes desarrollan e integran componentes de infraestructura deben conocer y tener claramente definidas sus responsabilidades por el uso de componentes sensibles de la misma.

Objetivos relevantes de COBIT

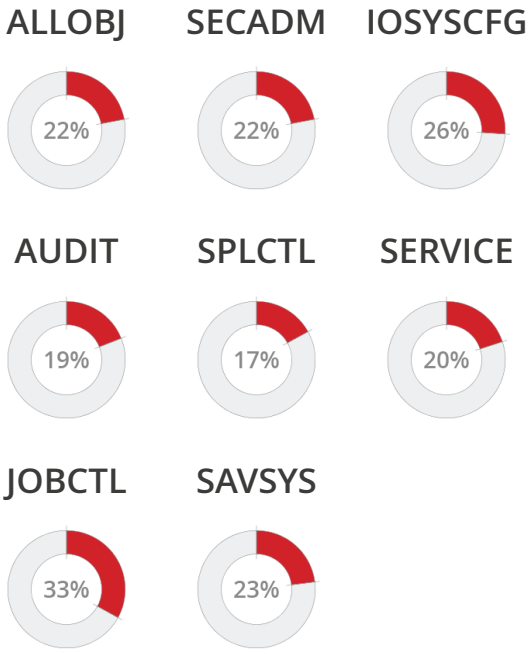
- COBIT DS5.3: - Gestión de Identidades
- COBIT DS5.4: - Gestión de Cuentas de Usuario
- COBIT AI3.2: - Protección y Disponibilidad de Recursos de Infraestrucura

Permiso especial *ALLOBJ

Un programador, desarrollador o administrador de bases de datos con permisos *ALLOBJ en un sistema productivo tiene acceso completo para hacer cambios a información sensible de las bases de datos. La segregación de funciones no se puede lograr si el personal de TI cuenta con permisos especiales en sus perfiles de usuario de uso cotidiano.

Umbral recomendado de cantidad de usuarios por cada permiso especial:

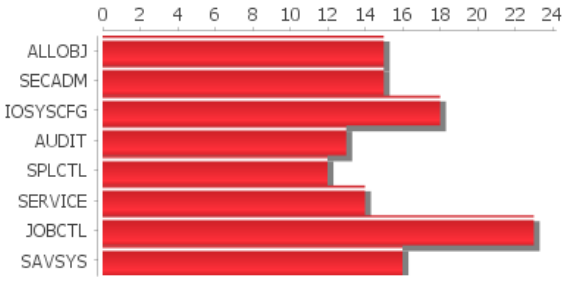
Porcentajes de usuarios con cada permiso especial:



Permisos especiales por encima de los umbrales recomendados:

8 DE 8

Cantidad de usuarios con cada permiso especial:



RECOMENDACIONES

Recomendaciones para el sistema

Estas recomendaciones provienen de validaciones de cumplimiento realizadas sobre el sistema. Haciendo uso de esa información, las recomendaciones se presentan ordenadas por prioridad, basándose en tres factores: riesgo de seguridad, tiempo de resolución y costo estimado.

1 Recomendaciones para Acceso de Usuarios

Asegure y monitorice las transacciones de red inmediatamente. - Este sistema IBMi está abierto al acceso desde cualquier PC en la red a través de diferentes servicios. Las transacciones PC-IBMi no se pueden rastrear ni controlar en estos sistemas. Este acceso de red es la mayor debilidad en la actual implementación. Recomendamos fuertemente controlar y monitorizar la actividad en la red y las acciones desde y hacia los sistemas IBMi. Actualmente, cualquier usuario con una PC y un ID de usuario puede acceder a todos los datos en el sistema a través de servicios de red y eludir la seguridad basada en menús.

PowerTech Network Securityes una solución líder de control de accesos para el sistema IBMi que permite monitorizar y controlar los accesos de red por medio de puntos de salida (exit points).

3 Recomendaciones para Seguridad por usuarios

Estándares de implementación de Seguridad por usuario - Este servidor no tiene estándares consistentes. Nosotros hicimos recomendaciones basándonos en la experiencia en la industria y estándares. En muchos casos, usted quizás deba desviarse de los estándares. En tales situaciones, recomendamos documentar cada desvío.

Perfiles de usuario inactivos - Hay 3 usuarios inactivos en el sistema (3 están habilitados). Elimine todos los usuarios inactivos del sistema.

Perfiles de usuario con contraseñas por defecto -7 perfiles tienen contraseñas por defecto (6 están habilitados). Reduzca la cantidad a cero y monitorice la creación de nuevos usuarios con esta condición.

5 Recomendaciones para Auditoría del Sistema

Establezca puntos de control para sus eventos de seguridad - Este sistema puede almacenar cientos de eventos de seguridad por día, pero no hay forma de ordenarlos o filtrar los eventos importantes y notificar a las personas adecuadas. Además, el sistema operativo no provee una forma de llevar control del tráfico TCP/IP como ODBC o FTP. Implemente una solución de seguridad y auditoría para IBMi que le permita responder: ¿Quién tiene permisos para qué? ¿qué eventos de seguridad son exposiciones de seguridad? ¿qué nuevas exposiciones se generan cada día?

PowerTech Compliance Monitor permite generar automáticamente en forma planificada reportes de auditoría personalizados para cada cliente.

6 Recomendaciones para Privilegios de Administración

Privilegios de administración: - Permisos especiales- Todos estos permisos especiales deben ser revisados y la cantidad de usuarios que gozan de ellos deben reducirse al mínimo. El criterio de otorgamiento de estos permisos debe documentarse. Una vez que se establecen los estándares, se debe monitorizar regularmente para detectar cualquier cambio.

PowerTech Authority Brokerpermite a las organizaciones reducir la cantidad de perfiles de usuario con permisos especiales. Los usuarios cambian a niveles de privilegio superiores solamente cuando es necesario y sus acciones quedan registradas.