

Seguridad en la plataforma Power i (AS/400)

¿Están sus datos asegurados? ¿Su negocio cumple con las normativas y regulaciones nacionales e internacionales en material de fraudes electrónicos? ¿Puede controlar su nivel de riesgo en material de seguridad IT?

Sabía Usted que las empresas están sometidas a cumplir una serie de regulaciones Internacionales; además las normativas de SOX, Basilea II, PCI, les demandan integridad y seguridad en los datos que manejan.

¿ Desea que sus sistemas estén protegidos y cumplir con las regulaciones?

Ahora puede estar tranquilo y seguro, Usted puede cumplir con las normativas y regulaciones nacionales e internacionales, puede disminuir el riesgo de fraude en sus sistemas Power i (AS/400), controlar todo tipo de acceso y obtener una Auditoría detallada.

La Suite IPSECURITY es la solución de Seguridad diseñada para obtener un completo alcance en la administración y cumplimiento de las regulaciones para las plataformas Power i (AS/400).

¡De un paso adelante! IPSECURITY además de apoyarlo en el cumplimiento de las regulaciones y normativas nacionales e internacionales le provee de todo un sistemas de Interfaz gráfico (GUI) que le ayudará a la detección rápida de cualquier actividad sospechosa en sus sistemas.

CARACTERISTICAS

PROTECCION MAXIMA DE POWER I:

Es una suite de seguridad que cuenta con controles de acceso de red, control de comando de AS/400 sobre usuarios como QSECOFR y auditorias en SQL y QRY. Los accesos externos puede ser controlados por IPSECURITY a través de los Exit Points, tenga usted el control de accesos hacia su Power i: Telnet, IFS, ODBC, FTP, DDM, etc.



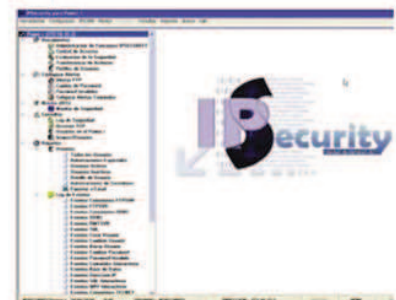
IDENTIFIQUE ACTIVIDADES SOSPECHOSAS

No subestime el riesgo de sufrir ataques directos, los fraudes, robo de información, delitos accidentales o incidentales son realizados por internos y externos a las compañías sin ser descubiertos, perdiendo valiosos datos, confiabilidad y rentabilidad.

LA AUDITORIA ES UNA NECESIDAD

Todo descontrol interno es una invitación a la pérdida de activos, los cuales pueden ser efectuados a través de los fraudes, en especial fraudes informáticos.

Las empresas pueden sufrir pérdidas todos los años por no seguir las normas y recomendaciones que genera una eficaz y oportuna Auditoría, además las normas ISO 17799 exige cumplimientos legales en términos de auditorías de control.





Sistema de SEGURIDAD Y AUDITORIA

INNOVACIONES TECNOLOGICAS

CONTROL DE COMANDOS INTERACTIVOS Y REMOTOS

IPSECURITY cuenta con un módulo para el control de comandos AS/400, con el que podrá restringir el uso de comandos de riesgos a cualquier perfil de usuario incluso a Super Usuario como QSECOFR sin afectar su operatividad.

DETENCION TEMPRANA: Con el módulo CSM (CENTRAL SECURITY MONITOR) podrá centralizar todos los eventos de seguridad de varios Power I (AS/400).

- Posibilidad de crear reglas de monitoreo.
- Proporciona informes para investigaciones de gran alcance para satisfacer estrictas exigencias de auditoría.

FACILIDAD DE USO: La suite IPSECURITY presenta una interfaz gráfica (GUI) que facilita la administración de la seguridad de los Power i (AS/400).

ALCANCE DE LA SEGURIDAD Y AUDITORIA DE SOLUCION IPSECURITY

TRAZABILIDAD DE MODIFICACIONES

- Nivel de Objetos
- Perfiles
- Valores de Sistema
- Autorizaciones, Attempts
- Full auditoria de la actividad de perfiles
- Transferencias a producción

DEFINICION DE REGLA

- Crea y adapta las reglas de la aplicación para generar auditorias definidas por el Usuario

CONTROL DE ACCESO

- ODBC, JDBC, OLE DB
- FTP, DATAQ, TELNET
- NetServer, IFS
- Net Print
- DDM, CMD 5250, RMTCMD
- iSeries Navigator

TRAZABILIDAD DE ACCESO

- Acceso a archivos sensitivos fuera de las aplicaciones
- Acceso a opciones de Menú

CONTROL DE TRAZABILIDAD DE COPIA

- CPYF
- CPYTOSTMF
- SAVOBJ
- CPYLIB
- CRTDUPOBJ

VALOR AGREGADO

Retorno de inversión, reducción del tiempo de administración y desarrollo invertido en la prevención de robo o uso indebido de datos y en la investigación de sucesos sospechosos. En resumen, la mejor solución de control y protección de acceso que puede obtener por su dinero.

IPSECURITY puede ser integrado al módulo IPS/JRN, para consolidar una auditoría a nivel de base de datos y sistemas.

Con la SUITE IPSECURITY, ¡De un paso adelante! Y comience ya a mitigar los riesgos en materia de seguridad de la información.



www.gt-supportusa.com / E-mail: contact@gt-supportusa.com
USA (305) 328.89.84

USA

7950 NW 53rd Street Suite 215 Miami, Florida



IPS/JRN de IPSECURITY

El módulo IPS/JRN es parte de la Suite de seguridad IPSecurity que le ofrece las soluciones de auditoría para el Power i (AS/400), que le permite auditar las Bases de Datos y el Journal de Auditoría del Sistema, el cual le apoyará en la identificación oportuna de las diversas vulnerabilidades que pudieran presentarse.

CARACTERISTICAS PRINCIPALES

- El módulo IPS/JRN cuenta con una interfaz gráfica que permite la evaluación en tiempo real de los eventos que atenten contra la seguridad, se ha desarrollado de tal forma que tiene un alcance deseado y apreciado por administradores y auditores de Seguridad. Cuenta con dos divisiones IPS/BD y IPS/AUD que se integran en la consola gráfica CSM (**Central Security Monitor**) para darle mayor monitoreo de Bases de Datos y Objetos.
- Monitoreo en Tiempo real, el módulo posee la facilidad para que los administradores programen las reglas de los eventos que desean auditar, con numerosas combinaciones de comparación a nivel de campos y objetos con operadores como : =, <, >, <>, >=, <= ; dándole al módulo un nivel de inteligencia de negocio para detectar eventos específicos y definidos por el usuario mediante una sintaxis de monitoreo que podrá alertar al administrador de posibles fraudes y accesos no permitidos a su datos y/u objetos.

Ej.: Podrá crear una regla donde especifique que al modificar el campo de límite de consumo en un archivo de crédito donde sea mayor a un determinado monto, se notifique inmediatamente al Administrador del Sistema.

IPS/BD

Provee de una auditoria a nivel de campo (base de datos), proporcionando un histórico donde se muestra los registro del **antes y después** de los cambios realizados a cualquier campo de sus archivos de bases de datos.

Permite tomar acciones inmediatas en tiempo real:

Ejecutar un programa y/o comando al momento que se produzca un cambio en la base de datos, le ayudará a evitar fraudes al momento que se realice la acción.

- Detección de las transacciones realizadas fuera de las aplicaciones administrativas del negocio.
- Monitoreo de campos vulnerables.
- Reporte detallado de modificaciones realizadas a cualquier tabla de BD.
- Envío de alertas vía SYSLOG, SMS, e-mail automáticamente y programables por evento.
- Reportes en formato PDF, HTML, e-mail, entre otros.
- Detección de modificaciones realizadas a la Base de datos del Power i as/400 mediante ODBC, JDBC, DDM, DRDA, entre otros.
- Auditoría continúa 24 horas al día y 7 días a la semana.
- Posibilidad de auditar de forma centralizada a través del CSM (CENTRAL SECURITY MONITOR) el cual posee la ventaja de visualizar toda la información de acciones y eventos de seguridad que se generen en todos los Power i de su empresa.
- **Fácil de usar, implementar y mantener**, la solución viene preconfigurada basándose en nuestro conocimiento de necesidades de seguridad.

IPS / AUD

Es el módulo de auditoría que cubre todas sus necesidades para el análisis en temas de seguridad a nivel de Objetos, Comunicaciones, Conexiones, Configuración, Valores de sistema y otros; posibilitando gestionar todos los eventos de seguridad en su empresa.

- Monitoreo de cualquier acción o evento en perfiles de usuarios, archivos, spool, valores de sistemas.
- Detección de intentos fallidos de autorización y cambio de autorizaciones sobre objetos.
- Permite crear reglas de auditoría de acuerdo a los requerimientos y necesidades de la empresa mediante pseudocódigos, donde podrá indicar que objeto, evento y usuario desea monitorear.
- Auditoría las 24 horas del día, los 7 días de la semana.
- Posibilidad de auditar de forma centralizada a través del CSM (**Central Security Monitor**) el cual posee la ventaja de visualizar toda la información de acciones y eventos de seguridad que se generen en todos los Power i de su empresa.
- Reportes en formatos PDF, HTML, Etc.
- Envío de Alertas via e-mail, SMS, SYSLOG.
- Real Time: posibilidad de ejecutar una acción en tiempo real, donde podrá ejecutar un comando, PGM al presentarse cualquier evento configurado por el administrador.