Libro blanco de Raz-Lee Security

Aplicación del marco COBIT para respaldar la ley Sarbanes Oxley y otras regulaciones de conformidad en el Servidor i de IBM

AH Technology escribió este libro blanco. AH Technology son distribuidores de iSecurity, un conjunto de productos de seguridad System i desarrollados por Raz-Lee Security

Ley Sarbanes Oxley

Contexto:

Sarbanes Oxley (SOX), COBIT (Objetivos de control para la información y tecnologías relacionadas)

La Ley Sarbanes Oxley (SOX) se promulgó en 2002 para tratar de evitar que se repitieran casos como los de Enron, Tyco, Worldcom y otras compañías estadounidenses similares.

El objetivo de la SOX es el de proteger a los inversores, mejorando la eficacia y fiabilidad de las revelaciones empresariales. La ley trae consigo sanciones criminales y civiles para las juntas de dirección ejecutiva, en el caso de que no se cumplan los requisitos exigidos por la ley. A tenor de lo dispuesto en el Artículo 404 de la ley, los ejecutivos tienen el deber de certificar y demostrar que han adoptado y mantienen una estructura y unos procedimientos de control interno adecuados para poder ofrecer la información financiera necesaria.

A pesar de que está claro que el espíritu de la ley es el de garantizar un nivel de seguridad e integridad de las empresas mucho mayor, la ley no es lo suficientemente transparente como para proporcionar un conjunto de directrices claras para la mediana empresa.

Muchos, en el campo de la Audit y la seguridad, recurren al desarrollo de las directrices bajo el nombre de Objetivos de control para la información y tecnologías relacionadas (COBIT®), desarrollados por el Instituto americano de gobierno del sistema informático (ITGI, por sus siglas en inglés) (www.itgi.org).

En su página web se menciona lo siguiente: "COBIT es un marco de gobierno y un conjunto de herramientas de apoyo informático que permite a los jefes llenar el hueco que existe entre los requisitos de control, cuestiones técnicas y riesgos empresariales. COBIT permite un desarrollo de política transparente y buenas prácticas dentro del control informático en todo tipo de organizaciones."

Política de conformidad y seguridad System i

El presente documento describe los objetivos de COBIT que consideramos más importantes para la seguridad, Audit y conformidad de System i. Cuando proceda, el documento ofrece referencias a las funciones iSecurity que pueden ser útiles a la hora de conseguir el nivel de conformidad necesario con COBIT (y de la misma forma con Sarbanes Oxley). Es recomendable que los usuarios de System i tengan acceso a la documentación de COBIT para
así poder valorar la lista completa de requisitos.

Sitios System i

El System i viene equipado con un importante número de herramientas de seguridad integradas en su sistema operativo. Dichas herramientas cubren áreas como la seguridad a nivel de objeto, registro integrado (Journals, incluido el Journal de Audit de seguridad, colas de mensajes, registro histórico, etc) y gestión integrada (colas de mensajes, etc).

El presente documento sólo hace referencia a los aspectos "técnicos" a la hora de aplicar las directrices. Existen muchos otros documentos que contienen sugerencias y recomendaciones sobre la aplicación de distintas metodologías disponibles para su puesta en marcha por parte de las empresas y para que de esta forma consigan el nivel de conformidad necesario.

Muchos sitios están usando software iSecurity como complemento de las herramientas System i nativas. En el presente documento se enumeran las cláusulas del COBIT más importantes, donde los usuarios pueden obtener beneficio del uso de iSecurity.

Resumen de los requisitos de la ley Sarbanes Oxley

IMPORTANTE

1. Exposición elevada (Véase el artículo que describe DS5.3)

En un caso en el que:

a. Un sistema System i tiene una aplicación ERP que permite a sus usuarios ver, copiar, cambiar y eliminar sus objetos (muchas aplicaciones de pantalla verde hacen esto)

y…

b. Es asimismo posible acceder al System i por medio de protocolos TCP/IP como FTP, SQL, ODBC, DDM y otros, haciendo uso de herramientas como MS Access, MS Excel, IBM System i Access etc (la mayoría de los sitios permiten este tipo de acceso).

Los datos de aplicación se pueden ver, copiar, cambiar o eliminar sin que el sistema operativo ofrezca ningún tipo de mecanismo para proteger, registrar o informar de dichas transacciones.

2. No-conformidad con la ley Sarbanes Oxley (Véase DS5.3)

Cuando una aplicación financiera se expone a lo anteriormente citado **NO CUMPLE con** la ley Sarbanes Oxley.

La ley Sarbanes Oxley dice claramente que un sistema TIENE QUE ser capaz de identificar cualquier intento de modificación de un registro financiero.

Tabla 1: Descripción de los objetivos COBIT y las funciones pertinentes de iSecurity

OBJETIVO COBIT	Descripción	Funciones de iSecurity que pueden aumentar la conformidad
DS5.1	Gestionar medidas de seguridad	Firewall, Password, Audit , Action, User Management, Visualizer
DS5.2	Identificación, Autenticación, Acceso	Firewall, Password, Audit , Action, User Management, Visualizer
DS5.3	Seguridad de acceso online a datos	View, Capture y Journal. También Firewall, Audit , Action para derivación y respuesta mejorada. Esta sección debe revisarse de manera inmediata debido a su impacto en los asuntos de no-conformidad.
DS5.4	Gestión de la cuenta de usuario	Password, User Management
DS5.5	Revisión de la gestión de las cuentas de usuario	Audit , Action, Assessment
DS5.7	Vigilancia de la seguridad	Firewall, Audit , Action, Capture
DS5.10	Informes sobre actividades y violaciones de seguridad	Firewall, Audit , Action
DS5.17	Protección de las funciones de seguridad	Firewall, Audit , Action, Antivirus
DS5.19	Prevención contra software dañino	Firewall, Audit , Action, Antivirus

DS5: ENVÍO Y ASISTENCIA – Garantiza la seguridad del sistema

DS5.1 Gestionar las medidas de seguridad

Este objetivo atiende a la necesidad de establecer una implementación informática de la seguridad que garantice que la política de seguridad y sus implementaciones cumplen satisfactoriamente con los objetivos empresariales y las exposiciones a posibles riesgos.

Este objetivo requiere no sólo la aplicación de la política de seguridad, sino también comprobaciones regulares para garantizar el continuo cumplimiento de la política de configuración del sistema.

Firewall, Audit y Action y Assessment iSecurity

1. El **Firewall** puede utilizarse para gestionar, controlar y proteger el acceso a los datos de la compañía desde todos los puntos TCP/IP de acceso al sistema (ODBC, FTP, SQL, System i Access, MS Access, MS Excel etc.). El **Firewall** puede registrar actividades aprobadas y rechazadas, generar informes, siempre que sea necesario, y, utilizando la interfaz con **Audit** y **Action,** enviar derivación inmediata mediante correo electrónico, SMS, etc, además de respuestas a amenazas en tiempo real.
2. El módulo de **Assessment de iSecurity** deberá actuar de manera regular, para así garantizar que la configuración del sistema no ha cambiado.

DS5.2: Identificación, Autenticación y Acceso

“La aplicación de una adecuada identificación, autenticación y autorización de los mecanismos deberá restringir el acceso lógico a y el uso de los recursos informáticos, haciendo de nexo de unión entre los usuarios y los recursos, con una serie de reglas de acceso. Dichos mecanismos deberán garantizar que el personal no autorizado, las conexiones de acceso telefónico y otros puertos de entrada (redes) del sistema no tienen acceso a los recursos del ordenador".

Firewall (incluido el gestor de Password), Audit y Action

1. Utilice el **Gestor de Passwords** y los valores OS del sistema para asegurarse de que los usuarios inactivos están desconectados; las Passwords varían regularmente y no es posible el uso de Passwords banales.

2. Utilice el **Firewall** para controlar todo aquello relacionado con el acceso de red TCP/IP (véase DS5.1), para de esta forma enviar una solución de protección contra intrusos (IPS, por sus siglas en inglés), mediante una Solución de detección de intrusos (IDS, por sus siglas en inglés) por parte de **Audit** y **Action** (derivación inmediata y respuesta a amenazas en tiempo real). La flexibilidad del **Firewall** permite configurar ciertas reglas para garantizar que sólo el personal autorizado tiene acceso a los datos sensibles (conectando una tarea a una dirección IP específica, prohibiendo el acceso a los datos desde fuera de la oficina, etc).

DS5.3: Seguridad de acceso online a datos

"La gestión informática deberá implementar procedimientos que estén de acuerdo con una política que proporcione controles de seguridad y acceso basados en la necesidad, demostrada por parte de los individuos, de ver, añadir, cambiar y eliminar datos".

Firewall (véase también respuesta a DS5.1, DS 5.2)

1. Este objetivo requiere que, en un entorno conectado en red, la seguridad esté implementada para que el acceso a los datos mediante el personal autorizado se haga de tal forma que, siempre que sea posible, se adopte el mayor nivel de granularidad para garantizar que el usuario pueda realizar sólo las tareas necesarias. Ejemplo: sólo lectura de datos, pero no actualización eliminación de los mismos.

2. Utilice el **Firewall** para controlar todo aquello relacionado con el acceso de red CP/IP (véase DS5.1), para enviar una solución de protección contra intrusos (IPS). El OS de System i permite una mayor granularidad, permitiendo al software que controle por separado diferentes acciones (verbos), como: LEER, ESCRIBIR, ELIMINAR, RENOMBRAR, CREAR OBJETO, CREAR BIBLIOTECA.

   PELIGRO: sin protección TCP/IP (por medio de software, como Firewall), su sistema **NO CUMPLE CON LA LEY SARBANES OXLEY** si se dan las siguientes condiciones:
   a. Cualquier usuario legal de la aplicación tiene autoridad para leer (ver), cambiar, copiar o eliminar registros de datos.
   b. La aplicación es una aplicación **financiera**.

   Sin protección de punto de salida TCP/IP, los usuarios que dispongan de la autoridad anteriormente citada pueden acceder para alterar registros financieros existentes. La Ley exige la habilidad para identificar cualquier intento de cambiar los registros financieros.

   La i5/OS nativa NO proporciona un mecanismo para gestionar, controlar y proteger datos contra transacciones TCP/IP (FTP, ODBC, SQL, DDM que utilizan herramientas como MS Access, MS Excel, IBM System i Access, FTP de DOS prompt, etc).

   PELIGRO: Si su aplicación financiera es una **aplicación de pantalla verde**, posiblemente su sistema **NO CUMPLA** con la ley.

3. Utilice **View** para esconder de manera selectiva registros completos de usuarios seleccionados o datos en campos seleccionados dentro de los registros, sin tener que hacer cambios en las aplicaciones. La interfaz GUI online se utiliza para definir criterios para esconder registros/campos.

4. Puede utilizar **Capture** para registrar imágenes de pantalla verde de la actividad de usuario. Dichas sesiones Capturedas pueden iniciarse como una disuasión de rutina o el módulo **Action** puede iniciarlas, tras la detección de una posible amenaza de seguridad, como el acceso a un archivo protegido o trabajo fuera del horario. Los registros de la sesión Captureda pueden archivarse a efectos legales y pueden buscarse más adelante si se establece que cierta información es sospechosa.

5. El **Journal** proporciona la capacidad de generar un informe de actividad de "línea temporal" histórico de una entidad en particular en una aplicación (número de cliente, número de hipoteca, etc), comparada a partir de todos los archivos de datos de System i, que constituyen la aplicación. El Journal proporciona una imagen anterior y posterior de los registros, ayudando así a la responsabilidad y rastreabilidad de los cambios y eventos de la aplicación.

DS5.4: Gestión de la cuenta de usuario
"El proceso de gestión deberá establecer procedimientos para garantizar acciones puntuales relacionadas con la petición, establecimiento, emisión, suspensión y cierre de las cuentas de usuario. Un procedimiento formal de aprobación que perfila el propietario del sistema o de los datos, garantizando la inclusión de los privilegios de acceso. La seguridad del acceso de terceras partes deberá definirse por contrato y afrontar los requisitos de la administración y los requisitos de confidencialidad. Los contratos de tercerización deberán afrontar los riesgos, controles de seguridad y procedimientos para los sistemas y redes de información en el contrato entre las partes."

User Management y Password

1. El proceso de gestión y el control de las cuentas de usuario deberán ser la piedra angular de la conformidad con la SOX. Con una política no muy estricta aunque sí factible, una compañía estará desnuda ante posibles abusos de usuarios al acecho de una oportunidad para dañar nuestro sistema.

2. Las funciones de Autenticación de usuario del proceso de **User Management** están destinadas a garantizar que un usuario es quien dice ser. Se han implementado en el System i medidas estilo PC de Windows, incluidas preguntas y respuestas personales, además de una Password de usuario única, generada por el sistema, desconocida incluso para el operador y el administrador del sistema. Esta Password tiene validez hasta que el usuario la cambia personalmente.

3. La función **Password**, en relación con este requisito, está relacionada con la centralización y facilidad de uso que ofrece el producto, para aplicar así los requisitos de Passwords de los sitios. La OS/400 nativa proporciona algunos de los valores importantes del sistema, aunque nunca dentro del contexto de un producto bien organizado. La **Password** asume todo aquello que le falta a OS/400.

DS5.5: Revisión de la gestión de las cuentas de usuario
"El proceso de gestión deberá contar con un proceso de control in situ para poder revisar y confirmar los derechos de acceso de manera periódica. Deberá llevarse a cabo una comparación de los recursos con la responsabilidad registrada, para ayudar a reducir el riesgo de errores o un cambio no autorizado."

Módulo de Assessment, Audit y Action iSecurity
1. Existen una serie de características **iSecurity** que se encargan de hacer frente a este requisito. Comience con el módulo de **Assessment iSecurity** para registrar sus ajustes actuales. Revíselo y cámbielos cuando sea necesario, cumpliendo así con sus objetivos comerciales y su política de seguridad. Vuelva a ejecutar la **Assessment iSecurity** y manténgala como referencia. De ahora en adelante, ejecute de manera regular el módulo de **Assessment iSecurity** y compare sus informes con su referencia.

2. Como medida complementaria, utilice **Audit** y **Action** para controlar todos los ajustes que puedan detectar (valores del sistema). Configure el software para derivar alertas cuando se cambie un ajuste.

DS5.7: Vigilancia de la seguridad

"La administración de la seguridad TI deberá garantizar que la actividad de seguridad queda registrada y que se informa de cualquier indicio de violación de la misma a todo el que corresponda, interna y externamente, y que se actúa de manera oportuna."

Firewall, Audit , Action, Capture

1. El **Firewall** garantiza que se informa de toda actividad TCP/IP y que queda registrada. Con **Audit** y **Action** se garantiza que cualquier intento de violación de la seguridad se transfiere de manera inmediata, llevando a cabo la Action correctiva o preventiva en tiempo real.

2. **Audit** y **Action** envían el mismo resultado cuando supervisan el Journal de Audit de seguridad, además de los eventos y mensajes del sistema.

3. **Capture** (véase 5.3.4, arriba).

DS5.10: Informes sobre violaciones y actividades de seguridad

"La administración de la seguridad TI deberá garantizar que cualquier actividad de seguridad o violación quede registrada, informada, revisada y transferida de manera adecuada y regular, para así identificar y resolver cualquier tipo de incidente relacionado con una actividad no autorizada. El acceso lógico a la información de responsabilidad de los recursos del ordenador (seguridad y otros recursos) estará garantizado, basándose en el principio del privilegio mínimo o necesidad de conocer.

Firewall, Audit y Action

1. Véase la información proporcionada en el aparatado 5.7. El **Firewall**, **Audit** y **Action** pueden proporcionar informes regulares, en cualquier intervalo de tiempo necesario, además de supervisión continua, detección inmediata, derivación y respuesta.

DS5.17: Protección de las funciones de seguridad

"Todo el hardware y software relacionado con la seguridad deberá estar protegido en todo momento contra su uso indebido para mantener su integridad y, asimismo, deberá estar protegido contra la revelación de claves secretas. Además, las organizaciones deberán guardar un perfil bajo sobre su diseño de seguridad, aunque no basarán sus seguridad en el secreto de su diseño."

Firewall, Audit , Action y Antivirus

1. Puede utilizar el **Firewall** para garantizar que ningún acceso no autorizado a través de la red pueda actualizar / eliminar / introducir datos en los archivos. El módulo **Antivirus puede llevar a cabo tareas de protección y detección de manera continua y puede eliminar los virus.**

DS5.19: Prevención contra software dañino

Detección y corrección

“En cuanto al software dañino, como los virus o troyanos, el proceso de gestión deberá establecer un marco de medidas de control correctivas, detectoras y preventivas adecuadas y una información y respuesta del suceso. La gestión empresarial e informática deberá garantizar que los procedimientos se establecen a lo largo de la organización para proteger los sistemas de información y la tecnología de posibles virus informáticos. Los procedimientos deberán incorporar protección y detección de virus y respuesta e información de suceso."

Antivirus, Firewall, Audit y Action iSecurity

1. Utilice el módulo **Antivirus** para garantizar que los virus y los códigos dañinos se detectan y eliminan lo antes posible.
2. El **Firewall** protegerá los ficheros de intentos no autorizados a través de la red de cambiar o eliminar datos.