Ley Sarbanes-Oxley – Controles de Acceso en TI – Un Enfoque Práctico

José Marcelino Acevedo Cruz
Postgrados – Especialización en Seguridad Informática
Universidad Piloto de Colombia
marcelino0709@outlook.com

Resumen- En este documento se contempla un marco general de la Ley Sarbanes-Oxley enfocada a los controles de acceso en TI y su implementación práctica en una Entidad, que busca mantener un nivel adecuado de seguridad en el acceso a las aplicaciones y estar preparado ante evaluaciones por parte de la auditoría interna como externa, sobre el cumplimiento de la citada Ley. Asimismo, muestra la relevancia de la participación de los Dueños de Proceso y del área de Seguridad de la Información en la verificación que en los sistemas de información se implementen opciones que sean acordes con las funciones que desempeñan los usuarios y que en la ejecución de las mismas exista una adecuada segregación de funciones, aspectos que son relevantes para certificación de cumplimiento con la Ley SOX que debe emitir el Presidente y el Vicepresidente Financiero de la Entidad.

Palabras clave- SOX, PCAOB, SEC, TI, Dueños de Proceso, área de Seguridad de la Información, Certificación.

Abstract- In this document it contemplated a general framework of the Sarbanes- Oxley Act focused on access controls in TI and its practical implementation in an Entity, with the objective to keep an adequate level of security for access to applications and be prepared before the evaluations by the internal and external audits, about the compliance of that Act. It also shows the importance of the participation of the Process Owners and the area of Information Security verifying that the information systems implemented options that are consistent with the roles of users and that there is adequate segregation of duties in implementing them, aspects that are relevant to certification of compliance with SOX law issued by the President and the Vice-president Financial Officer of the Entity.

Keywords- SOX, PCAOB, SEC, TI, Process Owners, area of Information Security, Certification**.**

I. INTRODUCIÓN

El cumplimiento de normativas tanto locales como internacionales (Ley SOX - Diminutivo para Sarbanes-Oxley, ley promulgada por el congreso de los Estados) así como la necesidad de contar con controles adecuados que aseguren la confidencialidad, integridad y disponibilidad de la información, hacen que las organizaciones desarrollen actividades, planeen e implementen proyectos encaminados a este objetivo y para esto se apoyan en empresas consultoras con quienes contratan soluciones de seguridad en Tecnología de la Información (TI), que les ayuden a definir reglas, marcos regulatorios y estándares que al implementarlos sustenten las políticas, les permita aplicar controles específicos de TI y poder demostrar que dichos controles están implementados y que operan de manera correcta [1].

En este documento, el lector encuentra información general que lo contextualiza acerca de la ley SOX y le da a conocer cómo es en la práctica la implementación en una compañía que debe dar cumplimiento a dicha ley, principalmente en lo que hace referencia a los controles de acceso en TI, la participación de Dueños de Proceso en la certificación de los accesos a los diferentes aplicativos, el apoyo del área de Seguridad de la Información en el monitoreo de los accesos y la generación de la información para las certificaciones, la evaluación por parte de las auditorías tanto internas como externas sobre el diseño y la efectividad de los controles implementados, y las acciones a realizar en casos de detectarse controles no operativos.

En la figura 1, se muestra un esquema del ciclo de vida del cumplimiento de la seguridad.

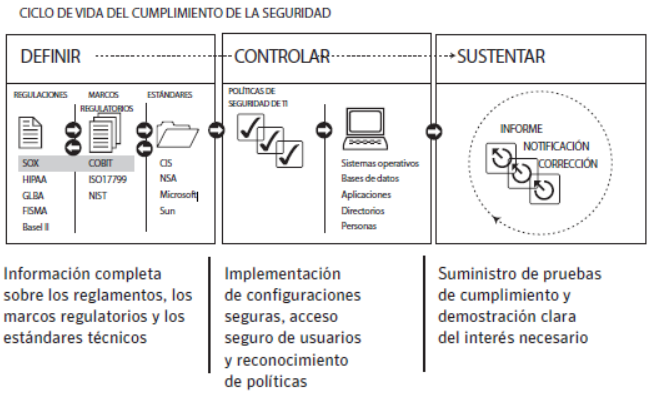


Figura 1. Ciclo de vida del cumplimiento de la seguridad. Fuente: http://eval.symantec.com/mktginfo/es/mx/enterprise/fact_sheets/DS-00431-SL_SOXreg_ds.pdf

II. GENERALIDADES

La Ley Sarbanes - Oxley fue promulgada en julio de 2002 con el objetivo de establecer nuevos y mejorados estándares para la contabilidad corporativa, el gobierno corporativo y la generación de reportes financieros, lo anterior como respuesta a los escándalos de fraude corporativos de finales de 1990. (Enron, Tyco International, WorldCom y Peregrine Systems).

El senador Paul Sarbanes y el congresista Michael Oxley reconocieron que se debía hacer un esfuerzo para probar a los inversionistas que sus intereses eran importantes, e impulsaron cada uno iniciativas que fueron conciliadas en un comité. El resultado de esta conciliación fue el "Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista" comúnmente llamada Ley Sarbanes-Oxley, SOX, SarbOx o SOA [2].

La Ley Sarbanes Oxley aplica a todas las compañías cuyas

acciones se encuentren registradas en las Bolsa de Valores de los Estados Unidos, como es el caso de algunas empresas colombianas entre las más importantes se encuentran Bancolombia, Avianca, Ecopetrol, Cementos Argos, ISA y Grupo Sura [3].

Para contextualizar al lector de este artículo, es importante darle a conocer el marco normativo existente alrededor de la Ley SOX, como son los roles que juegan la SEC y la PCAOB.

La SEC, es una comisión asociada al gobierno encargada de velar por el cumplimiento de la ley de mercado público de valores de Estados Unidos (Ley de 1993). El principal objetivo de la SEC es asegurase que los inversionistas tienen toda la información acerca de sus inversiones, para lo cual solicita a las entidades públicas información relevante sobre sus estados financieros.

La PCAOB, fue creada con la Ley SOX como una entidad privada que reporta a la SEC. Esta organización sin ánimo de lucro supervisa a los auditores de las compañías públicas. El propósito de la PCAOB es proteger a los inversionistas asegurando reportes de auditoría informativos e independientes. Esta función es ejercida mediante la certificación de las firmas de auditoría para auditar entidades registradas en la Bolsa de Nueva York, mediante la revisión de los papeles de trabajo del auditor independiente para evaluar el cumplimiento de las normas de auditoría y requerimientos de independencia establecidos en la Ley SOX.

Asimismo, es importante que el lector conozca las implicaciones de la Ley SOX establecidas en las secciones 302 y 404 de dicha ley.

En la sección 302, se establecen los procedimientos internos con el fin de asegurar la transparencia financiera, emitida a través de una certificación que firman el Presidente y Vicepresidente Financiero de la compañía. Se específica la responsabilidad penal que recae sobre la directiva de la empresa, ya que tienen que firmar informes sobre el aseguramiento de la veracidad de los datos que éstos contienen. Los funcionarios firmantes certifican que ellos son responsables. Esto es un cambio sustancial, ya que al menos hay una persona que firma y ante posibles irregularidades o fraudes esta persona firmante será la responsable.

En cuanto a la sección 404, la Ley SOX estableció nuevas responsabilidades para la alta dirección con respecto del establecimiento de un sistema de control interno, el establecimiento de mecanismos que aseguren la integridad de la información financiera, y evaluar la efectividad de la estructura de control interno y de los procedimientos. El marco de trabajo utilizado por la administración para evaluar la efectividad del control interno sobre reportes financieros es COSO. (Committe of Sponsoring Organizations of the Treadway Comission - COSO es un enfoque de control, requerido para cumplir con la Ley Sarbanes-Oxley) [4].

El Presidente y el Vicepresidente Financiero deben emitir una certificación relacionada con cada uno de los puntos mencionados anteriormente.

Teniendo en cuenta que el marco para evaluar la efectividad del control interno sobre reportes financieros es COSO, este artículo se centrará en los componentes que involucran controles de acceso en TI, como son: Información y Comunicación (controles sobre el acceso a información generada interna como externamente) y Actividades de Control (incluyen definiciones y controles sobre: aprobaciones, autorizaciones, revisiones de desempeño y segregación de funciones), los cuales están inmersos en la certificación de cumplimiento con la Ley SOX que al final debe emitir el Presidente y el Vicepresidente Financiero de la Entidad [5].

Por lo anterior, en este documento se relacionan los aspectos que son base para dicha certificación y están orientados a:

El papel que juegan los Dueños de Proceso en garantizar que los accesos otorgados a los usuarios corresponden con la funciones del cargo y la certificación que deben emitir sobre los accesos a los diferentes aplicativos; el área de seguridad de la información en el monitoreo de usuarios, roles y perfiles, y el apoyo de ésta área en la generación de la información para las certificaciones; las evaluaciones independientes de auditorías internas y externas sobre el diseño y la efectividad de los controles implementados, y las acciones a realizar en caso de detectarse desviaciones al momento de la evaluación operativa de los controles.

III. MONITOREO DE USUARIOS ROLES Y PERFILES POR PARTE DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN

Para el control de acceso a los sistemas de información, las entidades implementan procesos manuales y automáticos con miras a garantizar que el acceso a las opciones de las aplicaciones son acordes con las funciones que desempeñan los usuarios y que en la ejecución de las mismas, existe una adecuada segregación de funciones (una sola persona no hace una operación de principio a fin). Para llevar a cabo lo anterior, se apoyan en herramientas como las matrices de acceso a las aplicaciones y en procedimientos documentados tipo WorkFlow que describen los pasos para la solicitud de un usuario en una aplicación, la aprobación del acceso por parte del Dueño de Proceso y la implementación respectiva en el Sistema; sin embargo, este tipo de esquemas podría tener desviaciones originadas en la falta de validación por parte del Dueño de Proceso en cuanto a los roles y perfiles a asignar según las funciones a desempeñar por parte del usuario; o que si bien, los accesos solicitados correspondan, al momento de implementarlos hubiesen fallas.

Por lo anterior, se requiere de un monitoreo periódico de este tipo de procesos, con el fin de detectar de manera oportuna fallas en los procedimientos que generen una inadecuada asignación de accesos en los sistemas y por ende, inefectividad operativa de los controles SOX al momento de la evaluación por parte de las auditorías internas y externas.

En este aspecto, el área de Seguridad de la Información juega un papel importante, participando como apoyo a los Dueños de Proceso al momento de definir los roles y perfiles dentro de una aplicación, la cual se documenta en una matriz de acceso que se publica para consulta de los Dueños de Proceso y de los implementadores de acceso en los

aplicativos. La otra forma como participa el área de Seguridad de la Información, es como evaluador en el proceso de solicitudes e implementaciones de acceso, de tal forma que si alguna solicitud no corresponde con lo definido en las matrices de acceso, la solicitud se cancela; o si la falla se presenta al momento de la implementación del acceso por parte de los encargados, detectarla oportunamente y realizar los correctivos del caso.

En la figura 2, se muestra un ejemplo de cómo soportar un monitoreo:

MONITOREO SOLICITUDES DE USUARIOS

APLICACIÓN: INGRESOS

FECHA MONITORE	FECHA SOLICITUD	ROL SOLICITADO	CARGO	APRUEBA	ESTADO	OBSER.
02/02/2015	02/02/2015	AUXILIAR DE INGRESOS	AUXILIAR INGRESOS JUNIOR	Gerente Comercial de	Verificada	N/A
13/03/2015	13/03/2015	EJECUTIVO DE INGRESOS	ANALISTA PRINCIPAL	Gerente Comercial de	Cancelada	Rol no corres ponde
03/04/2015	03/04/2015	ANALISTA DE INGRESOS	ANALISTA PRINCIPAL	Gerente Comercial de	Verificada	N/A

Figura 2. Monitoreo de solicitudes de usuarios. Fuente: El Autor

IV. GENERACION DE CERTIFICACIONES DE ACCESO POR PARTE DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN

La generación de las certificaciones de acceso a los aplicativos, busca blindar el proceso de asignación de autorizaciones a los usuarios en los sistemas de información, ya que si bien los Dueños de Proceso son los encargados en primera instancia de autorizar a quiénes y con qué nivel dan acceso a la información de la cual son responsables, es posible que existan brechas en la asignación de roles y perfiles a los usuarios. Por lo anterior, el proceso realizado por el área de Seguridad de la Información para generar las certificaciones de acceso, le brinda tanto a los Dueños de Proceso como a los auditores internos y externos, una base confiable e independiente que soporta los accesos otorgados a los usuarios en los Sistemas de Información. La generación de las certificaciones se realiza con la periodicidad definida en la Entidad, que generalmente puede ser semestral y conlleva los siguientes pasos:

a) En la fecha de corte determinada del semestre, el área de Seguridad de la Información extrae directamente de los Sistemas de Información los reportes de usuarios, roles y perfiles correspondientes a las aplicaciones que se van a certificar y se agrupan por áreas Dueñas de Proceso, a quienes les va a ser remitidos. El reporte generado contiene la lista de usuarios de la aplicación a certificar, la fecha y la hora del último acceso del usuario al Sistema, el nombre del funcionario responsable del usuario, el rol que tiene el usuario dentro de la aplicación, y si el usuario se encuentra activo o inactivo.

   En la figura 3, se muestra un ejemplo de un reporte de usuarios, roles y perfiles.

LISTADO DE USUARIOS: APLICACIÓN DE INGRESOS

FECHA DE REPORTE: MAYO 29/2015 - 06:15:31 P.M.

USUARIOS	FECHA ULTIMO INGRESO	HORA ULTIMO INGRESO	DESCRIPCION DEL USUARIO	ESTADO
PP110101	29/05/2015	05:03:15 P.M.	Pepito Pérez - Auxiliar de Ingresos	ACTIVO
JJ120101	29/05/2015	05:30:16 P.M.	Jorge Jiménez - Analista de Ingresos	ACTIVO
MM130101	29/05/2015	05:00:00 P.M.	Manuel Molina - Ejecutivo de Ingresos	ACTIVO

Figura 3. Reporte de usuarios, roles y perfiles. Fuente: El Autor

b) El área de Seguridad de la información, es la encargada de la administración de las matrices de acceso, las cuales contienen la lista de opciones habilitadas en el sistema por cada uno de los roles definidos en las aplicaciones, así como los cargos autorizados por cada rol. Estas matrices son una herramienta importante para los Dueños de Proceso, ya que les permite de manera visual detectar la existencia de concentración de funciones en los cargos y al momento de ingresar un nuevo funcionario al área, les ayuda a determinar el rol adecuado según las actividades a desempeñar. Para el proceso de certificación, el área de Seguridad de la Información descarga las matrices de acceso de las aplicaciones, desde el sitio donde se publican, se seleccionan los roles y perfiles pertenecientes a cada área Dueña de Proceso y se envían a cada una de ellas. En la figura 4, se muestra un ejemplo de Matriz de Acceso

TÍTULO DEL DOCUMENTO: MATRIZ DE ACCESO DE INGRESOS VERSIÓN: 02 — **FECHA DE ACTUALIZACIÓN:** Marzo 31/2015

PERFILES

CARGOS: AUXILIAR DE INGRESOS JUNIOR
ROL : AUXILIAR DE INGRESOS
1 Registro de Operaciones
2 Consultas de Operaciones
3 Consulta de Saldos
4 Cuadre Diario
5 Preliquidar Operaciones
6 Imprimir
7 Reporte operaciones validación

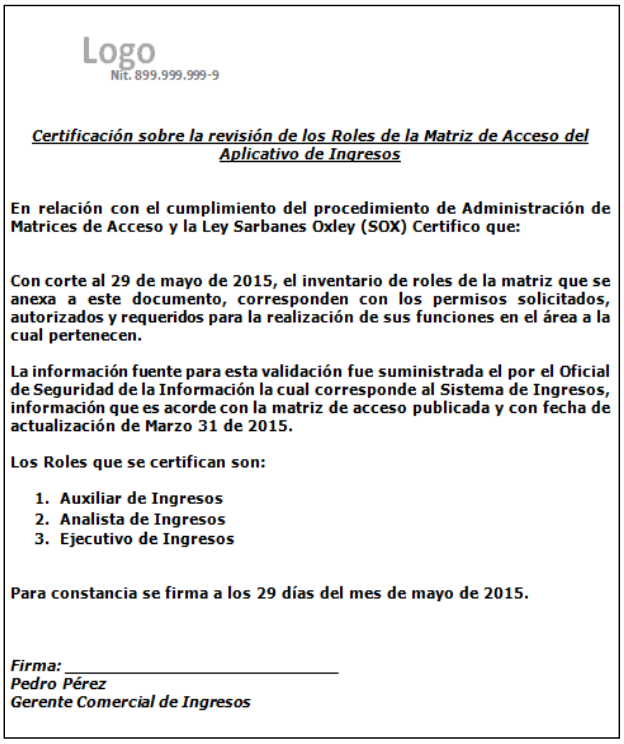
CARGOS: ANALISTA PRINCIPAL
ROL : ANALISTA DE INGRESOS
1 Consolidar operaciones
2 Conciliación diaria de operaciones
3 Validar reporte diario por Auxiliar
4 Solicitud autorización reversiones
5 Solicitud autorización montos
6 Consultas
7 Reportes

CARGOS: EJECUTIVO COMERCIAL
ROL : EJECUTIVO DE INGRESOS
1 Parámetros Monto por Operación
3 Autorizar reversiones
4 Autorizar operaciones por monto
5 Consultas
6 Reportes

CONTROL DE ACTUALIZACIONES		
FECHA	VERSION	NATURALEZA DEL CAMBIO
Ene. 2 / 2015	1	Creación de la Matriz
Mar. 31 / 2015	2	Actualización de Cargos por Rol, según autorización del 31 de marzo de 2015

Figura 4. Matriz de Acceso. Fuente: El Autor

c) El área de Seguridad de la información elabora en formato texto las certificaciones de acceso por cada Dueño de Proceso, para la firma respectiva, en la que se indica los roles de la aplicación a certificar, el corte con el cual se generaron los usuarios del Sistema y la fecha de actualización de la matriz de acceso que soporta los roles y perfiles definidos en la aplicación. En la figura 5, se muestra un ejemplo de una carta de certificación de acceso.



Logo
Nit. 899.999.999-9

Certificación sobre la revisión de los Roles de la Matriz de Acceso del Aplicativo de Ingresos

En relación con el cumplimiento del procedimiento de Administración de Matrices de Acceso y la Ley Sarbanes Oxley (SOX) Certifico que:

Con corte al 29 de mayo de 2015, el inventario de roles de la matriz que se anexa a este documento, corresponden con los permisos solicitados, autorizados y requeridos para la realización de sus funciones en el área a la cual pertenecen.

La información fuente para esta validación fue suministrada el por el Oficial de Seguridad de la Información la cual corresponde al Sistema de Ingresos, información que es acorde con la matriz de acceso publicada y con fecha de actualización de Marzo 31 de 2015.

Los Roles que se certifican son:

1. **Auxiliar de Ingresos**
2. **Analista de Ingresos**
3. **Ejecutivo de Ingresos**

Para constancia se firma a los 29 días del mes de mayo de 2015.

Firma: _____
Pedro Pérez
Gerente Comercial de Ingresos

Figura 5. Carta de Certificación de Acceso. Fuente: El Autor

d) A cada Dueño de Proceso le es remitido un paquete que contiene: los reportes de usuarios, roles y perfiles, las matrices de acceso de las aplicaciones a certificar y las cartas de certificaciones de acceso; cada una de ellas con el Vo. Bo. del área de Seguridad de la Información.
e) Se define un plazo para su revisión y firma, y en caso de existir ajustes, se revisan, ejecutan y se genera nuevamente el paquete para certificación. Es de resaltar, que si los ajustes corresponden a la asignación de opciones que no debían estar autorizadas a un usuario en el Sistema, el área de Seguridad de la Información debe validar que en los logs no se haya efectuado un uso indebido de las mismas.
f) Los paquetes de certificaciones de acceso los archiva el área de Seguridad de la Información y deben estar disponibles en el momento de ser requeridos por la auditoría interna o externa.

V. LOS DUEÑOS DE PROCESO Y LAS CERTIFICACIONES DE ACCESO

Los Dueños de Proceso son los encargados de:

a) Mantener los controles de los procesos de negocio y la información de tecnología asociada con las aplicaciones a cargo.
b) Mantener actualizadas las matrices Riesgo-Control de TI de los procesos a cargo.
c) Evaluar los riesgos con impacto financiero y determinar los controles para mitigarlos.
d) Determinar si los controles están bien diseñados y están operando.
e) Identificar las deficiencias de control interno del proceso.
f) Establecer los planes de remediación e implementarlos.

Teniendo en cuenta los roles y responsabilidades que tienen los Dueños de Proceso frente al cumplimiento de la Ley SOX, quienes tienen total responsabilidad por las matrices de Riesgo–Control de TI y por diseñar los controles y mantenerlos en operación efectiva, muchos de éstos apoyados en la tecnología; se hace relevante la especial atención que requieren los controles de acceso a los Sistemas de Información y es por esta razón que se requiere de su activa participación desde el momento de la definición de los roles y perfiles dentro de una aplicación y con el apoyo del área de Seguridad de la Información configurar los accesos según las funciones a desempeñar por parte de los usuarios, observando una adecuada segregación de funciones.

Una vez definidos los roles y perfiles dentro de una aplicación, los cuales se documentan como se mencionaba anteriormente en una matriz de acceso, le corresponde a los Dueños de Proceso velar porque los controles de acceso se mantengan en el tiempo y por lo tanto al momento de generarse nuevas solicitudes de acceso, deberá validar que los roles y perfiles a asignar dentro de una aplicación, correspondan con las funciones a desempeñar por parte de los usuarios y que no se genere conflicto de segregación de funciones.

Una vez el área de Seguridad de la Información genere las certificaciones con la periodicidad definida en la Entidad, que como se comentaba anteriormente puede ser semestral, los Dueños de Proceso con base en el paquete de información suministrado por el área de Seguridad de la Información, proceden de la siguiente manera:

a) Revisan los reportes de usuarios, roles y perfiles, frente a las matrices de acceso de las aplicaciones a certificar, con el fin de determinar que sean coincidentes.
b) Si la información es coincidente, validan directamente sobre el sistema de información y con los funcionarios a cargo, los accesos implementados en el sistema.
c) Si no se detectan brechas entre lo reportado por el área de Seguridad de la Información y la validación efectuada directamente sobre el Sistema, el Dueño de Proceso procede a firmar las cartas de certificaciones de acceso.
d) Si existen brechas, el Dueño de Proceso procede a solicitar a al área de Seguridad de la Información, el ajuste en la matriz de acceso y/o aplicativo según corresponda. Si se detectan ajustes relacionados con la asignación de opciones que no debían estar autorizadas a un usuario en el Sistema, solicita al área de Seguridad de la Información validar que en los logs no se haya efectuado un uso indebido de las opciones. Una vez recibido nuevamente el paquete para certificación, el

Dueño de Proceso procede a firmar las cartas de certificación de acceso correspondientes.

En la figura 6, se muestra un ejemplo de una matriz de Riesgo-Control del proceso de TI, en el cual se referencia el sub-proceso a cargo del Dueño de Proceso, el riesgo y la actividad de control que lo mitiga, el responsable de dicho control, el tipo de control (M/A – Manual o Automático, P/D – Preventivo o Detectivo), el procedimiento interno que soporta el control y la frecuencia de ejecución del control (Anual, mensual, semanal o diario). La carta de certificación y demás información soporte para la emisión de la certificación, se presentaron en el punto anterior.

Matriz Riesgo-Control
Proceso: TI
Sub-proceso: Accesos a programas y datos
Tipo de Control:
M/A - Manual o Automático
P/D - Preventivo o Detectivo
A - Frecuencia de Control Anual

Riesgo	Actividad de Control	Responsable del control	M/A	P/D	Ref. proced. Inter.	Frec. del control
Pérdida de confidencialidad de la información, por accesos no autorizados a aplicaciones.	Se tiene matriz de segregación de funciones por aplicación, administrada por seguridad	Oficial Seguridad y Dueños de Proceso	M	D	Procedimiento interno asociado al control.	A

Figura 6. Matriz Riego-Control proceso de TI. Fuente: El Autor

VI. EVALUACIONES INDEPENDIENTES DE AUDITORÍA INTERNA Y EXTERNA

Con las evaluaciones independientes realizadas tanto por la auditoría interna como externa, se busca que haya objetividad en la evaluación de la efectividad de la estructura de control interno en las Entidades y que sirva como soporte del cumplimiento con la Ley SOX. En la realización del proceso de auditoría se contemplan los siguientes aspectos: *las clases de evaluación de efectividad a controles, los métodos para realizar las pruebas, temas a tener en cuenta en la ejecución de pruebas, la documentación del resultado de las pruebas y el reporte de hallazgos.*

A. Clases de evaluación de efectividad a controles

Existen dos clases de evaluación de efectividad a controles [4] [6]:

a) Evaluación al diseño del Control: donde se valida si los controles realmente mitigan los riesgos sobre la información financiera identificados en los ciclos o procesos de negocio.
b) Probar la efectividad operativa del control: busca validar que los controles clave son ejecutados y operan para mitigar los riesgos de información financiera.

Con base en lo anterior, si un control a ser probado tiene una brecha de diseño (Gap), el control automáticamente falla, y no es necesario realizar la prueba de operatividad.

B. Métodos para realizar pruebas

Dentro de los métodos para realizar las pruebas, están [7]:

a) La Indagación, en la cual el auditor, debe tener en cuenta:
- Preguntar con ejemplos extremos sobre fallas de control.
- Indagar a más de una persona y si es necesario corroborar.
- Preguntar quién cómo, cuándo, dónde.
- Solo la indagación no provee suficiente evidencia de la efectividad del control.

b) La Observación, mediante la cual el auditor obtiene información:
- Observando a alguien ejecutar el control
- Es más confiable que la indagación.
- Le facilita el entendimiento de los procesos.
- Documenta quién, cómo y cuándo fue observado.
- Evidencia que el control opera en ausencia de documentación.
- Es útil para evaluar controles físicos.

c) Inspección / Examinación, permite:
- Inspeccionar documentación para validar el control.
- Obtener detalle para ser duplicado y verificar el resultado.
- Ser la vía más fácil y directa para obtener evidencia de la operatividad del control.
- Tener evidencias que pueden incluir explicaciones escritas, marcas de chequeo.

d) El Re-proceso:
- Provee mejor evidencia que las anteriores técnicas.
- Reprocesar el control y validar si se llega al mismo resultado de la persona ejecutora.
- Reconciliar utilizando fuentes de información independiente.
- Calcular independientemente procesos automáticos.
- Registrar transacciones hipotéticas y comparar los resultados.

C. Ejecución de pruebas

De los métodos mencionados anteriormente y para la evaluación de los controles de acceso en TI, que es el tema de este artículo, el auditor podrá seleccionar uno o una combinación de métodos orientados a la validación de los objetivos de procesamiento de información como son [8]:

a) Integridad: Todas las transacciones que ocurrieron son ingresadas para su procesamiento.
b) Exactitud: Las transacciones son registradas por el monto correcto, en la cuenta apropiada y en el periodo correcto.
c) Validación: Todas las transacciones registradas son reales y fueron aprobadas por el personal adecuado.

d) Acceso Restringido: La información es protegida ante accesos no autorizados, su confidencialidad es asegurada, y los activos físicos son protegidos.

En la figura 7, se presentan los controles clave en el procesamiento de información por cada uno de los objetivos antes relacionados.

OBJETIVO PROCESAMIENTO DE INFORMACION	DESCRIPCION DE LOS CONTROLES
Integridad	1) Transacciones registradas, ingresadas y aceptadas para procesamiento solo una vez. 2) Transacciones ingresadas y aceptadas para procesamiento en el archivo de datos apropiado. 3) Una vez que los datos son actualizados, éstos permanecen en el archivo correcto y vigente, y representan saldos
Exactitud	1) Datos clave registrados y ingresados por su monto correcto. 2) Cambios a datos existentes realizados por valores correctos.
Validación	1) Las transacciones han sido autorizadas 2) Las transacciones no son ficticias y son relativas al cliente. 3) Cambios de datos existentes son autorizados y no son cambiados sin autorización.
Acceso restringido	1) No se hagan cambios no autorizados a los datos. 2) La confidencialidad de los datos no fue vulnerada. 3) Protección de activos como efectivo e inventarios, se mantienen.

Figura 7. Controles clave en el procesamiento de información. Fuente: El Autor

En la ejecución de las pruebas, el auditor debe tener presente, que:

a) Entiende el control y el riesgo que éste mitiga.
b) Entiende qué es lo que demuestra que los atributos del control operan efectivamente.
c) Entiende los tipos de pruebas que va a efectuar (indagación, observación, inspección o examinación y reproceso).
d) Debe desarrollar los pasos de pruebas tal y como están definidos en el plan de pruebas.
e) Debe probar la totalidad de la muestra seleccionada sin considerar si existió una falla en alguno de los ítems probados.

Para la ejecución de las pruebas, el auditor puede apoyarse en formatos que lo guíen en el paso a paso. En la figura 8, se muestra un formato de plan de pruebas para la evaluación de controles del proceso de TI.

D. Documentación del resultado de las pruebas

Los resultados de las pruebas deben ser documentados de manera adecuada, de tal forma que la documentación debe ser suficiente para que cualquier persona con un conocimiento menor del control, pueda reprocesar la prueba sin ningún inconveniente. Es decir, si se probó una muestra de ítems, se deben registrar cuáles ítems fueron probados, y si por ejemplo se probó una definición del sistema, es importante mantener una impresión de pantalla del mensaje que se mostró en el momento de la prueba. Enmarcado en lo anterior, como mínimo los siguientes aspectos deben ser documentados en los resultados de pruebas:

a) Una descripción de la población de la cual se extrajo las muestras seleccionadas. Como evidencia es importante mantener las consultas realizadas en los sistemas.
b) La muestra seleccionada, incluyendo información específica del número de muestras seleccionadas.
c) El procedimiento de pruebas llevado a cabo, incluyendo un detalle de los pasos ejecutados para la ejecución de la prueba.
d) Los resultados obtenidos, indicando si ocurrieron o no excepciones; si ocurrieron excepciones, indicar cuándo y por qué se observó la excepción.
e) En la conclusión, indicar si se observaron o no, excepciones.

Los aspectos antes mencionados hacen parte del formato de plan de pruebas incluido en el punto anterior y la importancia de su correcto diligenciamiento, radica en que una falla en la documentación de una prueba puede ser evaluado como una potencial debilidad material (que afecta sensiblemente los intereses de la organización); al respecto, cuando a nivel de TI se detecte una deficiencia en un control, se debe determinar si existe un control o controles que compensen esa deficiencia para proteger a la organización y validar si los existentes mitigan efectivamente la deficiencia, o de lo contrario, optar por controles más apropiados [4].

EMPRESA: XXYY	
Formato de Prueba - Validación Efectividad Operativa	
Proceso:	**TI**
Sub-proceso:	**Accesos a programas y datos**
Ref. Control	**Código consecutivo del control**
Descripción Control:	**Se tiene una matriz de segregación de funciones por cada aplicación que es administrada por seguridad de la información**
Frecuencia:	**Anual, semestral, Trimestral**
Tipo de Control	**Detectivo o Correctivo**
Naturaleza del	**Manual o Automático**
Referencia a Procedimientos	**Procedimiento interno asociado al control**
Riesgo de control	***Alto***
Naturaleza de la Prueba	***Inspección - Examinación***
Pasos de la prueba:	**1. Solicitar el listado de las matrices de acceso . .** **2. Seleccione las matrices a revisar . . .** **3. Valide proceso de actualización . . .** **4. Identifique opciones que presentan**
Detalle de Criterios Evaluados.	
Criterios/Atributos	***Observ***
Muestra	
Ref. papel de trabajo	
Auditor	
Fecha de Prueba	
Revisor	
Existen Excepciones	
Numero de Excepciones	
Resultado validacion del	**No Ejecutado**
Conclusiones de la prueba y causas de la inefectividad	
Recomendaciones	

Figura 8. Formato Plan de Pruebas para Evaluación de Controles de TI. Fuente: El Autor

E. Reporte de hallazgos

Como base en las dos clases de evaluación de efectividad a controles, relacionados con el diseño del control y la efectividad operatividad del mismo, los hallazgos se clasifican de igual manera, así [4]:

a) Deficiencias de efectividad en el diseño: Una brecha de diseño existe si el control interno sobre reporte financiero no cumple efectivamente los objetivos de control para el cual fue diseñado y puede no prevenir o detectar errores o fraudes que puedan resultar en errores materiales de los estados financieros.
b) Deficiencia de efectividad operacional, también denominadas Excepciones, se clasifican así:
   - Hallazgo de documentación (D): El modo en el cual el control está documentado no da un entendimiento claro del control, y el hallazgo no fue identificado antes de que las pruebas iniciaran (por ejemplo en las pruebas de recorrido o en la planeación de las pruebas).
   - Hallazgo de evidencia (E): Olvidar evidencia de auditoría no significa que el control no esté operando efectivamente, pero indica que existe una debilidad de evidencia, que no le permite al equipo de pruebas confirmar con suficiente certeza, que el control está operando efectivamente.
   - Hallazgo de operación (O): es cuando un control no está funcionando tal como fue diseñado y/o el individuo que realiza el control, no tiene la autoridad necesaria y las competencias para ejecutar el control efectivamente.

En la figura 9, se muestra un formato de hallazgos en la evaluación de controles del proceso de TI.

Hallazgos identificados
Proceso: TI
Sub-proceso: Acceso a Programas y Datos
Tipo de Hallazgo
D - Documentación de Evidencia
E - Evidencia
O - Operación

Control	Descripción de la Defciencia	Tipo de Hallazgo	Recomendación Propuesta
Se tiene una matriz de segregación de funciones por cada aplicación que es administrada por seguridad de la información . . .	Brecha: No se identifica los posibles conflictos de segregación de funciones en la matriz de segregación de funciones . . .	D	Agregar en cada matriz de segregación de funciones de aplicaciones las opciones que presentan conflicto entre si . . .

Figura 9. Formato de Hallazgos Identificados. Fuente: El Autor

VII. PLANES DE ACCIÓN POR INEFICACIA DE CONTROLES

Identificados los hallazgos producto de las evaluaciones de auditoría, se procede con los planes de remediación. Los Dueños de Proceso deben trabajar en la identificación y documentación de los planes de remediación y para el caso del tema de este artículo, cuando la deficiencia identificada está relacionada con controles de acceso de TI, se apoyará en el área de Seguridad de la Información. Las actividades generales que contempla el plan de remediación, son las siguientes:

a) Los Dueños de Proceso deben priorizar las deficiencias y para esto:
   - Determinan cuáles son alcanzables (cómo y cuándo).
   - Determinan las actividades necesarias para que la remediación sea efectiva.
   - Implementan los correctivos correspondientes.
b) La auditoría procede a probar el control para validar que el control remediado opera efectivamente y procede así:
   - Ejecuta las pruebas una vez el Dueño del Proceso le haya informado de la corrección de las deficiencias.
   - En la ejecución de las pruebas deberá tener en cuenta que haya suficiente tiempo para probar su operatividad.

En la figura 10, se muestra un formato de planes de acción para los hallazgos producto de la evaluación de controles de acceso en TI:

Plan de Remediación a Hallazgos identificados
Proceso: TI
Sub-proceso: Acceso a Programas y Datos
Tipo de Hallazgo
D - Documentación de Evidencia
E - Evidencia
O - Operación

Descripción de la Defciencia	Tipo de Hallazgo	Recomendación Propuesta	Aclarado con	Fecha de Aclaración	Comentario de la Gerencia	Prioridad
Brecha: No se identifica los posibles conflictos de segregación de funciones en la matriz de segregación de funciones . . .	D	Agregar en cada matriz de segregación de funciones de aplicaciones las opciones que presentan conflicto entre si . . .	José Jiménez - Oficial de Seguridad.	Mayo 25 de 2015	De acuerdo, se procede a actualizar matriz.	BAJA

Figura 10. Formato Planes de Acción. Fuente: El Autor

VIII. CONCLUSIONES

Contextualizados en lo relacionado con la Ley SOX y la importancia de establecer un sistema de control interno, con mecanismos que aseguren la integridad de la información financiera, así como la evaluación de la efectividad de la estructura de control interno, se observa la relevancia de los controles de acceso en TI como apoyo para certificación de cumplimiento con la Ley SOX que debe emitir el Presidente y el Vicepresidente Financiero de la Entidad.

Asimismo, se mencionó que la existencia de un adecuado control de acceso, ayuda a garantizar que en los sistemas de información se implementen opciones que sean acordes con las funciones que desempeñan los usuarios y que en la ejecución de las mismas exista una adecuada segregación de funciones. Sin embargo, teniendo en cuenta que los controles son ejecutados por personas, cabe la posibilidad de fallas en la validación por parte del Dueño de Proceso al momento de la definición o autorización de los roles y perfiles a un usuario, o que si bien los accesos solicitados estén bien definidos, al momento de implementarlos hubiesen fallas.

Planteado lo anterior, se requiere de un monitoreo periódico de este tipo de procesos, con el fin de detectar de manera oportuna fallas en los procedimientos que generen una

inadecuada asignación de accesos en los sistemas y por ende inefectividad operativa de los controles SOX al momento de la evaluación por parte de las auditorías internas y externas.

En síntesis, es difícil contar con controles infalibles, por lo que es importante en todo proceso contar con controles complementarios o compensatorios, que mitiguen el riesgo de inefectividad operativa de los mismos.

REFERENCIAS

[1] Symantec, "Cumplimiento de la ley Sarbanes-Oxley". Agosto de 2006. [Online]. Disponible: http://eval.symantec.com/mktginfo/es/mx/enterprise/fact_sheets/DS-00431-SL_SOXreg_ds.pdf

[2] Wikipedia, "Ley Sarbanes Oxley". Agosto de 2012. [Online]. Disponible: http://es.wikipedia.org/wiki/Ley_Sarbanes-Oxley

[3] Portafolio, "Este es el club de firmas colombianas en Wall Street". Enero de 2014. [Online]. Disponible: http://www.portafolio.co/economia/firmas-colombianas-wall-street

[4] Santiago Campuzano Vallejo – Juan Fernando Jaramillo, "Impacto de la Ley Sarbanes-Oxley a la Seguridad de los Sistemas de TI". Noviembre de 2008. [Online]. Disponible: https://repository.eafit.edu.co/xmlui/bitstream/handle/10784/2740/Jaramillo_JuanFernando_2008.pdf?sequence=1&isAllowed=y

[5] Pricewaterhouse Coopers, "Marco Integrado de Control Interno COSO 2013 – Alcaldía de Medellín - Secretaría de Evaluación y Control". Noviembre de 2014. [Online]. Disponible: https://www.medellin.gov.co/irj/go/km/docs/pccdesign/SubportaldelCiudadano_2/PlandeDesarrollo_0_20/Publicaciones/Shared%20Content/Documentos/2014/SEMControlAuditoriaInterna/COSO%202013%20-%20Marco%20Integrado%20de%20Control%20Interno_V2.pdf

[6] Jaime Alejandro Safra Gutiérrez, "Metodología para Evaluar la Efectividad del Diseño y Operación de los Controles en la Realización de Auditorías Basadas en Riesgos". Febrero de 2011. [Online]. Disponible: http://www.bdigital.unal.edu.co/3972/3/98559963.2011.pdf

[7] Norma Internacional de Auditoría 500 (NIA-ES 500) "Evidencia de Auditoría. Adaptada para su aplicación en España mediante Resolución del Instituto de Contabilidad y Auditoría de Cuentas". Octubre de 2013. [Online]. Disponible: http://www.icac.meh.es/NIAS/NIA%20500%20p%20def.pdf

[8] ISACA, "COBIT - Objetivos de Control para la Información y Tecnologías Relacionadas". Junio de 2014. [Online]. Disponible: http://www.isaca.org/cobit/pages/default.aspx