UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

AUDITORÍA DE EVALUACIÓN DEL MODELO DE CONTROL DE TECNOLOGÍA DE INFORMACIÓN PARA CUMPLIMIENTO DE LA LEY SARBANES OXLEY, EN UNA EMPRESA PRIVADA DEL SECTOR FINANCIERO COSTARRICENSE

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios del Posgrado en Administración y Dirección de Empresas para optar al grado y título de **Maestría Profesional en Auditoría de Tecnologías de Información**

SUSTENTANTE:

André Martínez Campos

A83717

Ciudad Universitaria Rodrigo Facio, Costa Rica

Mayo 2018

DEDICATORIA

A mi madre, por su respaldo incondicional y ser mi mayor admiración.

A mis abuelos, tíos y hermano, por su amor y presencia.

A Dios, por acompañarme a lo largo del camino.

AGRADECIMIENTOS

A la empresa, por confiar en mí y permitirme realizar este trabajo.

A mis compañeros, por hacer más amena la travesía y los cursos del proyecto.

A la persona que con su paciencia y apoyo me impulsa a crecer profesionalmente.

A todos aquellos que de una u otra manera me han permitido llegar hasta aquí.

HOJA DE APROBACIÓN (Proyecto Final)

Este trabajo final de investigación aplicada fue aceptado por la Comisión de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información.

Magister Gino Ramírez Solís

Profesor – Coordinador

Magister Alejandro Zúñiga Gómez (Profesor UCR)

Tutor-Lector

M.Sc. María José Araya Quesada

Lectora–Empresa

M.Sc. Ridiguer Artavia Barboza

Director Programa de Posgrado en Administración y Dirección de Empresas

André Martínez Campos

Sustentante

TABLA DE CONTENIDOS

LISTA DE GRÁFICOS

LISTA DE FIGURAS

RESUMEN EN ESPAÑOL

Este documento contiene la ejecución de un ejercicio cuyo objetivo fue aplicar una auditoría al diseño y efectividad de los controles establecidos por la gerencia de Tecnología de Información para el cumplimiento de la ley Sarbanes Oxley. Derivó en una opinión sobre los controles definidos y generó las oportunidades de mejora pertinentes, con el fin de asegurar su eficacia y dar una seguridad razonable de la mitigación de los riesgos respectivos relacionados con TI.

Como parte del alcance, se abarcó un total de tres controles de la cartera definida para TI en la organización, por medio de la ejecución de una prueba de escritorio, una prueba de recorrido del control y una prueba de validación de su efectividad.

Asimismo, se generaron los machotes de papeles utilizados en el ejercicio y se adjuntó dicha información con el objetivo de proporcionar una guía para futuros esquemas de trabajo similares.

A nivel de resultados, se evaluaron tres controles en alcance, los cuales resultaron con una conclusión de "Adecuado en diseño", y dos controles que se declararon como "Inefectivos en ejecución", lo cual implicó la recomendación al respecto.

Como parte de las recomendaciones, se generaron diez oportunidades de mejora, orientadas a evitar posibles inefectividades futuras y a mejorar la gestión a nivel de las áreas encargadas.

RESUMEN EN OTRA LENGUA DIFERENTE AL ESPAÑOL

This document contains the execution of an audit exercise to comply with the Sarbanes Oxley act, the auditor gave an opinion on the design and effectiveness of the defined controls and develops the corresponding improvement opportunities.

The objective of the work was to apply an audit to the design and effectiveness of the controls established by the administration in order to comply with the Sarbanes Oxley act, to ensure its effectiveness and provide reasonable comfort on IT risk mitigation.

As part of the scope, three controls of the portfolio defined for IT were included, executing a desk test, a walkthrough test and an effectiveness validation test.

Likewise, guidelines were generated, and information is attached to provide a guide for similar future work schemes.

As a result, the audit evaluated three controls; and obtained three with a conclusion of "Adequate in design" and two controls that were declared as "ineffective in execution" which implied the election in this regard.

As part of the recommendations, ten opportunities for improvement were generated, which can prevent future ineffectiveness and improve management.

Nomenclatura

Nemónico	Definición
TI	Tecnologías de Información
PT	Papel de Trabajo
BD	Base de datos
TFG	Trabajo Final de Graduación
UCR	Universidad de Costa Rica
CGR	Contraloría General de la República
NIA	Normas Internacionales de Auditoría
SOX	Ley Sarbanes Oxley
TESTING	Prueba de auditoría

CAPÍTULO 1- INTRODUCCIÓN

Este documento incluye un ejercicio de auditoría SOX en una institución financiera del sector privado costarricense. A continuación se detalla la distribución de su contenido.

En el capítulo uno se encontrará la definición del alcance, la justificación del proyecto y la definición del problema por resolver. En el capítulo dos se definirá el objetivo general y los objetivos específicos, así como la metodología que se utilizará para ejecutar todo el proceso. En el capítulo tres se presenta el programa de trabajo para las etapas de ejecución y cierre del proyecto, así como una descripción de las etapas finales. En el capítulo cuatro se ubican los machotes de papeles de trabajo que se generaron para la asignación. Seguidamente en el capítulo cinco se encuentran los resultados del trabajo realizado. Y finalmente, el capítulo seis contempla las conclusiones acerca de la experiencia del ejercicio y recomendaciones generales de la práctica profesional.

1.1 Objetivos

OBJETIVO GENERAL:

Aplicar una auditoría al diseño y efectividad de los controles establecidos por la gerencia de Tecnología de Información para el cumplimiento de la ley Sarbanes Oxley, con el fin de asegurar su eficacia y dar una seguridad razonable de la mitigación de los riesgos respectivos relacionados con TI.

OBJETIVOS ESPECÍFICOS:

1. Validar la razonabilidad de que el control interno de la entidad financiera salvaguarda la estructura y el esquema establecido por el sistema financiero costarricense.
2. Realizar y documentar la evaluación independiente del diseño y efectividad de los controles, de acuerdo con el plan de trabajo aprobado por el comité de Auditoría.
3. Diseñar documentos que sirvan como base para futuras evaluaciones de cumplimiento con la ley SOX en entidades financieras.

1.2 Alcance

A pesar de la existencia de una matriz del proceso IT que contiene 55 controles, la auditoría se enfocará en las áreas de seguridad y continuidad de negocio, las cuales, a nivel de materialidad, se consideran críticas con respecto a la declaración de la matriz. Esta incluirá los siguientes controles SOX en el alcance:

- ITSOX014 –Seguridad de la Accesos a Sistemas.
- ITSOX015 –Cambios en parámetros de seguridad.
- ITSOX019 –Pruebas de restauración de información.

Dentro de las áreas en alcance se encuentran el área de Seguridad de Sistemas y de Productividad y Eficiencia.

Asimismo, la población por evaluar es la que comprende el período julio – diciembre 2017 y la auditoría se aplicará de enero a abril de 2018.

1.3 Justificación

La ejecución de una evaluación del diseño y la efectividad de controles SOX permitirá a la organización conocer el estado actual de los controles que mitigan los riesgos con respecto a la generación de estados financieros con información errónea o alterada, cuya probabilidad es atacada por medio de controles de Seguridad de Sistemas y Continuidad de TI.

Dentro de la estructura de control interno es importante que las evaluaciones independientes emitan una opinión acerca de la definición y el cumplimiento de los procedimientos definidos. Lo anterior porque con esta auditoría se espera mejorar el sistema de control y verificar la efectividad y eficacia de la operación de las salvaguardas definidas, así como su alineamiento con los riesgos de la organización.

A nivel personal, la auditoría permitirá la aplicación de los conocimientos adquiridos durante la maestría profesional de Auditoría de Tecnologías de Información y agregará valor a la empresa en un proceso sumamente importante de cumplimiento regulatorio. A partir del estudio se espera que las recomendaciones sirvan para solventar irregularidades o riesgos identificados.

1.4 Marco metodológico

1.4.1 Clasificación de la investigación

El presente trabajo, según Barrantes Echeverría (1999) se clasifica de la siguiente manera: se considera una investigación **aplicada,** se aplica el conocimiento adquirido durante la maestría a un caso real en una institución costarricense, con la finalidad de detectar aspectos sujetos a mejora en el control interno del lugar que se analiza. El estudio realizado no pretende aportar un conocimiento teórico nuevo al campo de la Auditoría sino atacar potenciales problemas generadores de riesgo en el tema evaluado, que en este caso es el cumplimiento de la normativa Sarbanes Oxley en una institución financiera del sector privado costarricense.

Se considera en su **alcance temporal** como una investigación **transversal o sincrónica**, ya que se realiza en un momento específico (enero-abril 2018) y los datos o situaciones analizadas también pertenecen a un periodo determinado (julio-diciembre de 2017).

Según su **profundidad u objeto,** se puede catalogar como **descriptiva,** ya que se trata de una condición encontrada, que se valora contra unos criterios normativos establecidos que rigen el tema evaluado, tanto a nivel interno como externo (ámbito costarricense), y de ahí se emiten los aspectos de mejora.

Respecto de su enfoque o medición se considera **cualitativa,** ya que se describirán situaciones ordinarias de la institución evaluada sin cuantificar o manipular datos numéricos específicos, más que los que se observan o responden en instrumentos cualitativos. Tiene lugar en el **campo** y no en un laboratorio, con situaciones naturales y libertad de acción de los observados.

La **validez** de la investigación radica en la evidencia que recaba el postulante durante su trabajo de campo y el debido proceso de ejecución. La **confiabilidad** se ampara en el diseño de los instrumentos denominados como ***"Papeles de Trabajo"*** que se basan en la normativa (interna y externa), estándares, criterio experto y mejores prácticas en el campo evaluado.

1.4.2 Detalle de metodología e instrumentos a utilizar

Para iniciar con el marco metodológico se considera pertinente definir los siguientes dos conceptos: método y técnica.

Método: es la manera de ordenar una actividad, orden sistemático que se impone en la investigación, camino para llegar a cierto resultado, que se compone de varias técnicas (Barrantes, 1999).

Técnica: es un conjunto de instrumentos de medición, elaborados con base en los conocimientos; puede ser de medición o de recolección de la información (Barrantes, 1999).

La auditoría se va a realizar en una institución perteneciente al sector privado. Se realizará con base en la metodología para realizar auditorías SOX indicada en el documento *"Manual operativo Pruebas de efectividad SOX"*, que es de acatamiento obligatorio para la organización, cuyas etapas se describen de la siguiente manera:

Planificación:

1. Asignación de pruebas y entendimiento del control

El auditor interno recibe de parte de la jefatura del área, el cronograma de pruebas a aplicar durante la ejecución del presente proyecto. Este cronograma contiene información básica de los controles asignados (Matriz a la que corresponden, referencia del control, referencia control anterior, entre otra información). Adicionalmente, detalla la versión del consolidado de matrices con la cual se deben evaluar los controles y que serán también utilizadas en el presente proyecto.

Luego de extraída la información se consideran los siguientes elementos antes de realizar la prueba.

Actividad de control

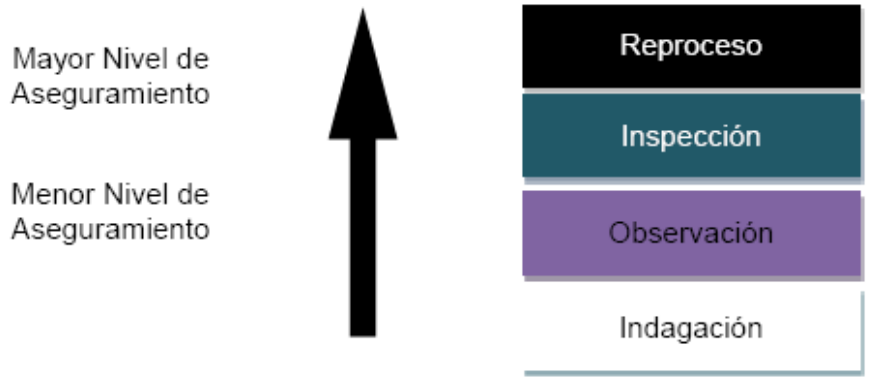
El auditor o postulante realiza un entendimiento del control a evaluar por medio de la lectura de la actividad de control y de ser necesario mediante entrevista al área responsable.

Naturaleza de la prueba

De acuerdo con la técnica usada, las pruebas se clasifican en cuatro categorías: indagación, observación, inspección y reproceso. Algunas de estas técnicas, se utilizarán en este proyecto considerando aquellas que provean mayor aseguramiento. De igual forma podrían utilizarse la combinación de dos o más de ellas.

Figura N°1

Niveles de aseguramiento



Fuente: Manual operativo Pruebas de efectividad SOX.

- **Indagación:** está técnica busca determinar si el control se está ejecutando según el diseño, mediante la realización de preguntas, orales o escritas, sobre quién, cómo, cuándo y dónde se ejecuta el control. Asimismo, busca obtener información acerca de los errores identificados utilizando ejemplos sobre situaciones de falla de control que se pudieran presentar. Es importante mencionar que la indagación, por sí sola, no provee suficiente evidencia de la efectividad del control y se requiere de su combinación con otra de las técnicas.

- **Observación:** esta técnica implica observar la ejecución del control. Es más confiable que la indagación y facilita el entendimiento de los procesos. En ausencia de documentación, permite evidenciar que el control opera y es útil para controles como arqueos, inventarios físicos de títulos, etc.

- **Inspección:** está técnica requiere inspeccionar documentación para validar el control y es la vía más fácil y directa para obtener evidencia de la operatividad del control. La evidencia puede incluir explicaciones escritas o marcas de chequeo.

- **Reproceso:** provee mayor evidencia que las anteriores técnicas. Implica reprocesar el control y validar si se llega al mismo resultado alcanzado por la persona que lo ejecuta, reconciliar utilizando fuentes de información independiente, calcular independientemente procesos automáticos o registrar transacciones hipotéticas y comparar los resultados.

Naturaleza del control

La extensión de las pruebas para un control en particular varía dependiendo de varios factores, incluso de si es un control automático o manual.

- **Pruebas de controles automáticos:** para controles automáticos, el número de ítems a probar puede ser mínimo (uno o muy pocos ítems), siempre que los controles de TI hayan sido validados y sean efectivos.

- **Pruebas de controles manuales**: las pruebas de controles manuales deben incluir una mezcla de las técnicas de auditoría mencionadas anteriormente. Una validación independiente efectiva requiere la inspección de la documentación que soporta la ejecución del control; y para mitigar el riesgo de que no se identifiquen errores, se debe seleccionar un número apropiado de ítems a ser probados (referidas como "muestras"). El tamaño de las muestras se basa en el juicio y nivel de aseguramiento que la gerencia espera obtener y según las tablas o lineamientos remitidos.

Frecuencia del control y nivel de riesgo (tamaño de la muestra):

Con base en la frecuencia del control y al nivel de riesgos, se selecciona el tamaño de la muestra a evaluar, cuyo método de selección siempre es **aleatorio.**

El tamaño de la muestra definido por la administración se basa en la importancia del control y en el nivel de aseguramiento deseado, cuando existe un número menor de ítems probados aumenta el riesgo de una conclusión incorrecta. Por lo anterior, se debe considerar el mayor número de ítems para aquellos controles altamente críticos o cuando el control provee el mayor soporte sobre la validez de una manifestación en una cuenta con materialidad significativa.

Adicionalmente, debe existir una clara fuente de la extracción de la población, de preferencia de forma independiente.

La selección de la muestra debe quedar documentada en la hoja de muestra e incluida en los papeles de trabajo.

Solicitud de la información (población o evidencia) para la ejecución de las pruebas:

Se solicitará la evidencia por vía correo electrónico a las áreas con un correo dirigido al dueño del control, enlace y jefatura del área en caso de no responder en el tiempo establecido (2 días) a la Gerencia de Área. Dentro del mismo correo se debe indicar que el responsable contará con dicho tiempo para la entrega de la información, excepto casos debidamente justificados, tales como recepción de expedientes en archivos físicos donde el área realiza la aclaración y la solicitud del tiempo.

2. Confección de la prueba (Desarrollo del testing)

En la evaluación de efectividad, luego de realizado el entendimiento y tipo de control y seleccionada la forma de evaluarlo, se procede con la aplicación del *testing* definido. Para esto, es importante validar que sea adecuado para la evaluación de la actividad de control descrita, dado que los controles pueden variar de una versión a otra de la matriz.

Según la actividad de control existen diferentes tipos de pruebas, entre ellas:

Pruebas de accesos:

Se refiere a pruebas que verifican la efectiva asignación de accesos a un sistema según la descripción de la actividad de control. Estos deben probarse en un 100% con base en la información obtenida de la fuente del sistema en revisión.

Pruebas operativas:

Se refiere a pruebas que verifican el cumplimiento de determinado procedimiento según la descripción de la actividad de control.

Pruebas de controles automáticos

Se refiere a pruebas que comprueban en sitio el funcionamiento de determinado sistema o su correcta parametrización para determinado proceso.

La confección de la prueba debe quedar documentada en la plantilla de pruebas de efectividad. Por medio de un Excel independiente por prueba.

Ejecución

3. Conclusión de la prueba

Todo plan de pruebas deberá tener una conclusión de la efectividad operativa del control. La conclusión de la efectividad solo puede ser calificada entre "Efectivo" o "Inefectivo"; en los casos donde se califique como "Inefectivo" se debe describir de manera detallada la deficiencia de control identificada, incluida una explicación de cuál es el riesgo de error o fraude sobre la información financiera.

Todas las pruebas de resultado inefectivo serán discutidas con el dueño del control, y el dueño de proceso y debe firmar en señal de aceptación de la brecha, de igual forma el auditor que efectuó las pruebas. Esto por medio de documentación física o correo electrónico (con acuse de recibo) y deberá adjuntarse la captura de pantalla al pie de la plantilla de la prueba.

La conclusión tanto efectiva como inefectiva debe contener los siguientes elementos mínimos:

- Debe ser integral y específica (asociación de la mitigación del riesgo-control-prueba). No deben repetirse los atributos revisados, ya que estos quedan explicados en el procedimiento de la prueba y en la sumaria respectiva.
- Debe explicar cómo el auditor llegó al criterio emitido (Efectivo o Inefectivo).
- Debe contener datos numéricos (estadísticos) de los resultados (cuando aplique). Por ejemplo: de los 50 (100%) usuarios con acceso a la opción de parametrización de cuentas, 10 (20%) usuarios no cumplen con el perfil del puesto establecido en la actividad de control.
- Debe quedar redactada de la misma forma en que un hallazgo normal de auditoría.

4. Documentación papeles de trabajo

A continuación, se detallan algunos puntos que se consideran al momento de documentar las pruebas en los papeles de trabajo:

- Los procedimientos seguidos deben quedar debidamente detallados y con su respectiva evidencia incluyendo la documentación soporte.
- Todos los archivos anexos deben adjuntarse de forma clara y ordenada ayudando al lector a comprender la información, bajo la opción de Insertar-Objeto.
- Para la selección de la muestra se debe documentar la fuente de información, población total, la herramienta utilizada para la selección. El archivo ‘’Muestra’’ descrito en el punto número uno de este documento debe insertarse en el papel de trabajo como evidencia.
- Todos los ítems probados deben quedar en un 100% respaldado.

5. Pruebas de diseño:

Se utiliza la metodología de análisis de controles en escritorio y recorrido, con la que se busca confirmar si los controles están debidamente diseñados para prevenir o detectar oportunamente, errores materiales sobre las cuentas y revelaciones significativas.

Los tipos de evaluación se describen de la siguiente manera:

Escritorio:

Se evalúa a través del procedimiento de indagación y permite evaluar y determinar si:

- Las cuentas y procesos relacionados están dentro del alcance de materialidad de SOX para los estados financieros de la organización.
- De materializarse el riesgo podría afectar los resultados de los Estados Financieros (por error o fraude).
- El control mitiga las aserciones del riesgo descrito.
- Determinar si los controles cubren las aserciones relevantes del riesgo descrito.

Los pasos a evaluar son:

1. Tomar la información relevante (subproceso, riesgo, control, si el mismo es manual o automático) de la última versión de las plantillas: 'Matriz de Riesgo y Controles' y 'Calificación del Riesgo'.
2. Evaluar si los riesgos identificados son clave dentro del proceso contable. De materializarse el riesgo podría afectar los Estados Financieros (por error o fraude); si eso ocurre se deben seleccionar las aserciones que se pueden ver afectados.
3. Evaluar si los controles identificados son claves dentro del proceso contable, ya que mitigan el riesgo definido.

Resultados de la revisión de escritorio

Lo primero que se debe hacer es determinar si la cuenta está dentro del alcance de materialidad; en caso contrario ahí se detiene la evaluación.

Si la cuenta está dentro del alcance, los incumplimientos serán reportados como deficiencias en el diseño y debe establecerse un plan de remediación inmediato que contemple lo siguiente:

- Que el control mitigue un riesgo clave operativo pero no contable (aserciones incorrectas por error o fraude).
- El control no mitiga el riesgo de las aserciones.
- Los controles no cubren todas o parte de las aserciones relevantes del riesgo descrito.

Revisión del recorrido: En esta etapa se contempla la verificación de los siguientes aspectos:

- La redacción del control está conforme al control aplicado.
- El control mitiga el riesgo identificado.
- La frecuencia del control permite identificar un error oportunamente.
- La persona que ejecuta el control cuenta con el conocimiento y la experiencia requerida.
- Existe una segregación de funciones en el inicio, autorización, procesamiento, contabilización, reporte y control de las transacciones.
- Las excepciones resultantes de ejecutar el control son resueltas oportunamente.
- La información utilizada para realizar el control es confiable.

Resultados de la revisión de recorrido

Si como resultado de la evaluación del diseño se identifican incumplimientos en los aspectos del control antes mencionados, tales serán reportados como deficiencias en el diseño. Entonces debe establecerse un plan de remediación inmediato en dos vías posibles, a saber:

- Recomendación de Control: implica el riesgo no se encuentre cubierto por un control o se requiere de un control complementario para mitigar el riesgo residual.

- Ajuste al control: si bien existe un control, se requieren ajustes para mitigar el riesgo (ej. periodicidad, ejecutor, información utilizada).

Como parte del análisis de recorrido, el auditor debe realizar una evaluación del nivel de riesgo para cada control. Para ello debe responder a una serie de criterios y, a su vez,

comparar el nivel de riesgo resultante con el asignado por la administración según la matriz de controles.

Comunicación

6. Comunicación de resultados

Toda inefectividad que resulte de la aplicación de una prueba debe ser comunicada de la siguiente manera:

- Pruebas de controles automáticos validadas en sitio: la comunicación se realiza al momento de ejecutar la prueba y determinar su inefectividad; posteriormente, se hará la evaluación de la inefectividad con la gerencia de auditoría y se comunicará al responsable de control por medio de un correo electrónico enviado al enlace indicado en el consolidado de matrices con copia al Gerente de área.
- Para pruebas en las que no exista necesidad de validar en sitio primero, se debe realizar la validación de la inefectividad con la gerencia de auditoría o la jefatura del área; posteriormente se realiza la comunicación mediante correo electrónico enviado al responsable del control, al enlace indicado en el consolidado de matrices y con copia al Gerente de área.
- Adicionalmente, se efectuará una conferencia con la gerencia y el lector de empresa, para exponer los resultados y emitir los documentos de aprobación del proyecto (acta de conferencia y oficio de conformidad).

Instrumentos diseñados en cada etapa

Planificación

- **Programa de trabajo:** es un documento formal que se utiliza como guía metodológica en la realización del trabajo. El programa indica la descripción de actividades a desarrollar de acuerdo con un orden y una lógica, y dentro de un periodo o tiempo determinado.

Ejecución

- **Plantillas de trabajo de revisión de diseño y efectividad:** son papeles de trabajo para evaluar o describir condiciones encontradas, listas de chequeo, cuadros resúmenes de información recopilada, resultados de pruebas, hojas de recolección de hallazgos, etc.
- **Diseño del Informe Borrador:** se diseña el informe borrador, para la aprobación.
- **Informe definitivo:** debe incorporar las observaciones o recomendaciones que la administración haga a cada hallazgo, si lo evidenciaron suficientemente.

Comunicación

- **Acta de reunión de comunicación de resultados:** contiene los datos de fecha, hora, inicio y fin; participantes convocados y presentes (con firma); observaciones y comentarios con nombre completo y puesto.
- **Recibido conforme de la institución:** documento emitido por la misma persona que autorizó la realización del evento con firma de la persona contacto (cuando fuese diferente). En este se indica el cumplimiento de lo acordado y el grado de satisfacción con el trabajo.

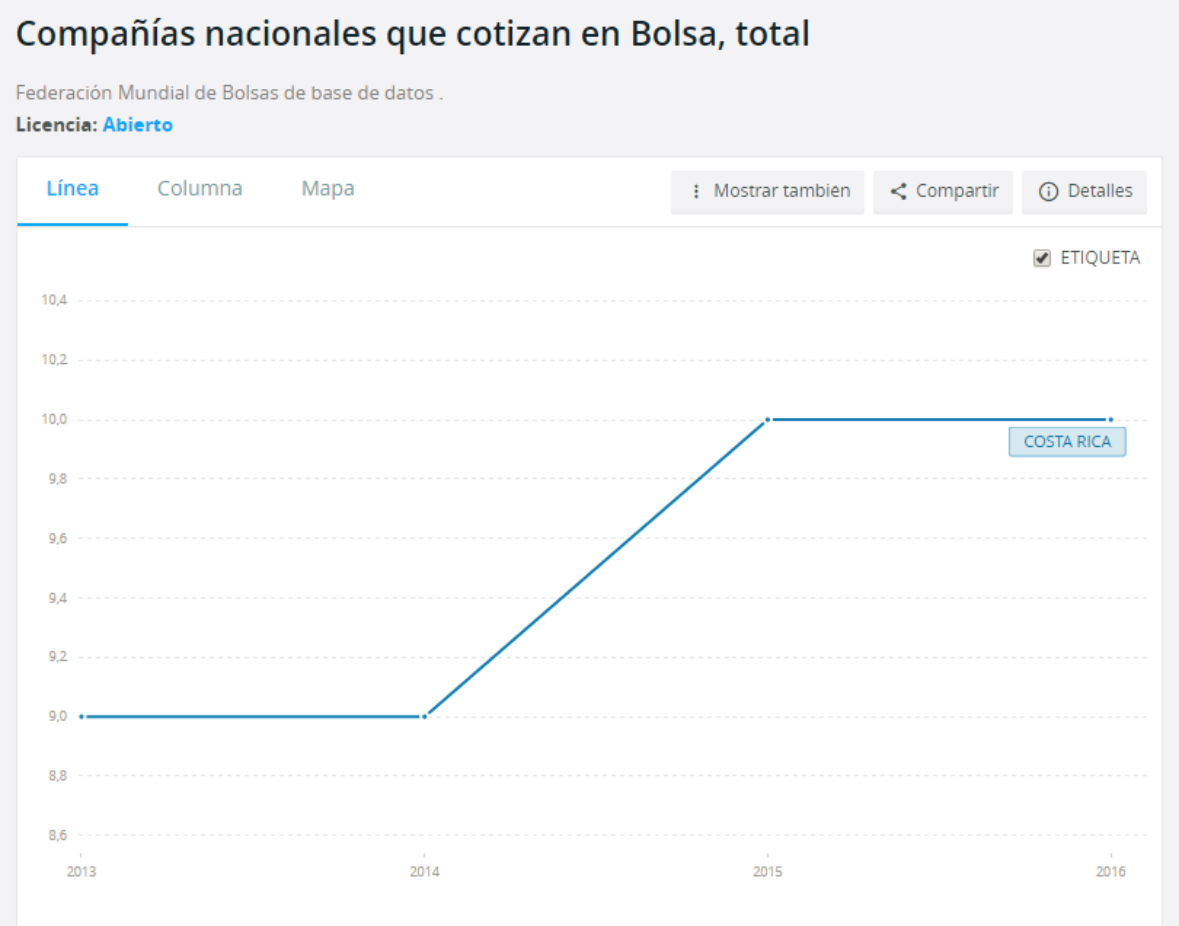
CAPÍTULO 2- PERSPECTIVAS TEÓRICAS

2.1 Estado de la cuestión en Costa Rica.

En Costa Rica, el mercado bursátil externo es limitado y generalmente son las transnacionales quienes deben cumplir con normativas internacionales aplicadas a inversores de bolsas específicas, como es el caso de la ley SOX.

El siguiente gráfico muestra la cantidad de organizaciones que actualmente se encuentran registradas a nivel país en la bolsa de Nueva York.

Gráfico # 1



Fuente: Banco Mundial.

Es así como este tipo de proyectos ayudan a agilizar el proceso de maduración de las empresas costarricenses y la protección de la información utilizada para generar los estados financieros. De esta forma se evitan casos como el de Yanber, donde la presentación de información falsa llevó al sistema financiero a otorgar créditos sin la garantía respectiva, exponiendo la economía del país.

2.2 Historia de la empresa donde se desarrollará el proyecto

Los inicios de la institución financiera se remontan a más de medio siglo atrás, cuando en 1952 se fundó una institución financiera en Nicaragua. Sin embargo, no fue sino hasta los años setenta cuando se incursionó en el negocio de tarjetas de crédito.

A mediados de los años ochenta, la empresa decidió ingresar en otros mercados de la región, empezando por Costa Rica. Fue en la década de 1990 cuando se concretó la expansión hacia los otros mercados centroamericanos, fortaleciendo así la presencia en toda la región, la cual se mantiene hasta la actualidad.

Ya en el año 2004 se iniciaron las operaciones de tarjeta de crédito en México, y un año más tarde se llevó a cabo una alianza estratégica por medio de la cual una empresa extranjera adquirió el 49,99% del capital.

Paralelamente y como parte de la estrategia de expansión, se llevó a cabo la adquisición de un banco privado muy importante en Honduras. En el 2007 también se adquirieron instituciones dirigidas a segmentos específicos de mercado en El Salvador y en Costa Rica.

A mediados del 2009 la empresa extranjera aumentó su participación accionaria al 75% y se convirtió así en el accionista mayoritario. No obstante, a raíz de un cambio de estrategia a escala mundial, decide concentrarse más en la actividad industrial (infraestructura, tecnología y salud) y menos en actividades de banca privada y comercial.

Como resultado, en julio del 2010 un conglomerado financiero suscribió un contrato de compraventa de acciones con la empresa extranjera relativo a la adquisición del 100% de las acciones. En diciembre del 2010, y después de obtener las aprobaciones de las superintendencias de entidades financieras de cada país, el proceso de compra culminó exitosamente.

Cabe resaltar que, a pesar del cambio de control accionario, la estrategia de negocios y la identidad de la institución financiera se mantienen y, a raíz de la adquisición, ha sido posible ofrecer productos de mayor valor agregado a los clientes, compartir experiencias, aprovechar las sinergias y las mejores prácticas de ambas partes, y, sobre todo, compartir la visión de negocios. Todo eso que hace que la organización sea caracterizada por el mejoramiento continuo, la pasión por la excelencia, la innovación y la creatividad.

Misión

Facilitar con excelencia el intercambio y financiamiento de bienes y servicios, a través de sistemas de pago y soluciones financieras innovadoras y rentables que contribuyan a generar riqueza, a crear empleo y a promover el crecimiento económico sostenible y solidario de los mercados donde operamos.

Visión

Ser la organización financiera preferida de todas las comunidades que servimos por nuestra conectividad con personas y empresas, por nuestra confiabilidad, espíritu innovador, solidez y claro liderazgo en los sistemas de pago de la Región.

A nivel de control interno, en la organización se perciben las siguientes características:

- Presencia de áreas dentro de las gerencias encargadas del control interno y el seguimiento y atención de auditorías.
- Existencia de una gerencia de Calidad, orientada a la ejecución de auditorías en los procesos y la recomendación de oportunidades de mejora en los mismos.
- Existencia de certificaciones de calidad a lo largo de procesos del grupo, que permiten estandarizar la operativa y establecer la documentación pertinente de cada caso.
- Existencia de un área de Riesgo que acompaña a las áreas en la mitigación y el establecimiento de controles, así como la atención de eventos.
- Existencia de un área de Auditoría Interna que se encarga de la ejecución de revisiones operativas, regulatorias, financieras, de procesos, de Tecnología de Información y así de enfoques integrales que mezclan los tipos anteriores.
- Presencia de una estructura de gobierno corporativo conformada por comités que analizan temas relativos a la estrategia o al apetito de riesgo de la organización.

2.3 Normativa asociada

Por ser un banco del sector privado, y según la normativa internacional de las organizaciones que cotizan en la bolsa de valores de Nueva York, la organización debe cumplir con la ley Sarbanes Oxley (en adelante Ley Sox), la cual es la mayor reforma realizada por los mercados financieros de Estados Unidos desde la ley de Mercado de Valores de 1934 que fue proclamada en julio de 2002, principalmente en respuesta a escándalos contables que involucraron a importantes compañías en Estados Unidos. Estos escándalos resultaron en una falta de confianza en los mercados financieros y en las prácticas contables y de reporte.

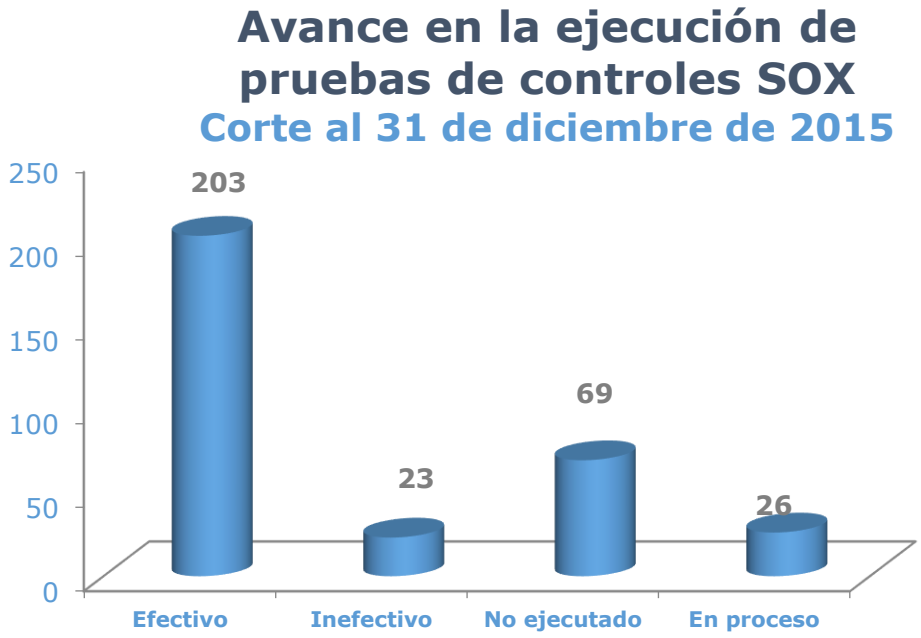
En junio de 2003 entró en vigencia la Sección 404 de la Ley Sox de 2002, la cual requiere que la administración de las compañías registradas ante la Securities and Exchange Commission - SEC (compañías públicas) evalúe anualmente si el control interno sobre reporte financiero ("ICFR" por sus siglas en inglés) es efectivo.

La Sección 404 de la Ley Sox estipula que las compañías públicas deben responsabilizarse por mantener un sistema de control interno sobre el reporte financiero que genere un aseguramiento razonable sobre la confiabilidad de la información financiera y la preparación de los estados financieros para propósitos externos, de acuerdo con principios de contabilidad generalmente aceptados. En este sentido, la administración es responsable de mantener evidencia, incluida la correspondiente documentación, que provea un soporte razonable a su evaluación. Esta evidencia le permitiría a un tercero, como es el auditor externo de la compañía, basarse en el trabajo realizado por la administración para soportar su evaluación de la efectividad del control interno en cumplimiento de la Sección 404.

2.4 Estudio preliminar

En el estudio preliminar, posterior a investigar los temas por tratar, se determinó que, en el periodo 2015, Auditoría Interna realizó la revisión de controles SOX de julio a diciembre. En esta fase se efectuó una estadística cuyos resultados se exponen a continuación:

Gráfico #2



Fuente: Informe Auditoría Interna.

De un total de 321 controles, 203 tuvieron resultado efectivo, 23 inefectivos, 69 no ejecutados (se probaron entre enero y marzo) y 26 que se encontraban en proceso por algún tema de suministro de información.

Con base en los resultados arrojados en la fase de 2015, se considera necesario una validación de cumplimiento y evaluación del diseño de los controles para la mitigación de los riesgos relacionados, y determinar la situación actual de los mismos.

CAPÍTULO 3- DESARROLLO DEL TEMA DE INVESTIGACIÓN

Como parte del proceso de auditoría, se iniciará una etapa de planificación que definirá los procedimientos por realizar en la fase de ejecución, la cual se estructura de la siguiente manera:

3.1 Actividades de una auditoría de TI

Tal como se planteó en la metodología, la investigación abarca tres grandes macroetapas: Planificación, Ejecución y Comunicación de resultados. A continuación, se describe cada una de ellas:

3.1.1 Etapa 1- Planificación

Esta etapa inicia con un estudio preliminar para definir claramente el objetivo y la naturaleza de la empresa, así como para conocer las necesidades y el ambiente de control donde se desarrolla la auditoría.

Producto de la anterior indagación se determina la oportunidad y posibilidad real de llevar a cabo el trabajo con el alcance y en el tiempo establecido, así como los recursos requeridos.

Una vez determinada la viabilidad de cumplir con los objetivos del proyecto y de la empresa, se prepara el programa de ejecución del trabajo, para que cuando esté aprobado se comiencen a determinar las áreas de riesgo, diseñar las herramientas para poder atender de extremo a extremo todo el programa de ejecución, diseñar el mapa de riesgos, las pruebas, los cuestionarios, las guías de entrevista y todas las plantillas de trabajo para evidenciar su ejecución.

3.1.1.1 Programa de examen del proyecto

En esta etapa se diseña el programa para la actividad de planificación, en el que se definan los procedimientos de auditoría que se requieren aplicar para cumplir con los objetivos correspondientes a esta actividad, así como el objetivo, naturaleza, alcance, oportunidad, plazo y responsables de su ejecución (CGR, 2014).

En virtud de lo anterior, se describe a continuación el programa para ejecutar la auditoría de evaluación de controles SOX.

Proceso a Auditar	Diseño y efectividad de controles SOX		
Responsable:	André Martínez Campos		
Aprobado por			
	Magister Alejandro Zúñiga	**Firma**	**Fecha**
	Magister Gino Ramírez	**Firma**	**Fecha**
Plazo de ejecución	De enero a marzo de 2018		

1. Objetivos de la auditoria

Aplicar una auditoría al diseño y efectividad de los controles establecidos por la Gerencia de Tecnología de Información para el cumplimiento de la ley Sarbanes Oxley, con el fin de asegurar su eficacia y dar una seguridad razonable a la mitigación de los riesgos respectivos.

2. Naturaleza

La presente auditoría se realiza como proyecto de graduación para obtener el grado de Magister en Auditoría de Tecnologías de Información del Programa de Posgrado en Administración y dirección de Empresas de la Universidad de Costa Rica.

3. Alcance

Dentro del alcance se incluirán los siguientes controles SOX:

- ITSOX014 –Seguridad de la Accesos a Sistemas.
- ITSOX015 –Cambios en parámetros de seguridad.
- ITSOX019 –Pruebas de restauración de información.

4. Procedimientos de trabajo

Procedimientos a ejecutar			
ID	Detalle	Ref. PT	Tiempo estimado
1	Realice la revisión de escritorio de los controles en alcance con el fin de verificar la adecuada mitigación del riesgo de los controles, la idoneidad de la persona que lo ejecuta y la integridad de la información que se procesa.	F-Prueba de diseño	3 días
2	Consiga la muestra para la revisión de recorrido de los controles en alcance con el fin de obtener los elementos por probar.	F-Prueba de diseño	2 días
3	Ejecute la revisión de recorrido para los controles con el fin de verificar el cumplimiento con los controles en alcance declarados e identificar desviaciones en el proceso.	F-Prueba de diseño	1 semana
4	Obtenga la muestra para la revisión de efectividad de los controles en alcance con el fin de obtener los elementos por probar.	F-Prueba de efectividad	2 semanas
5	Ejecute la revisión de efectividad de los controles en alcance para cada elemento de la muestra, verificando la evidencia generada como soporte del control y la ejecución de las actividades declaradas en la matriz de controles, con el fin de verificar el cumplimiento de procedimientos.	F-Prueba de efectividad	3 semanas
6	Diseñe el informe borrador y envíelo a su aprobación	Informe Borrador	3 días

7	Emita el Informe definitivo y convoque a reunión	Informe definitivo	1 día
8	Conferencia de cierre	Minuta de reunión de cierre	1 día

3.1.2 Etapa 2- Ejecución

Esta etapa parte de lo definido en la planificación para desarrollar la auditoría. En una fase inicial se estructuraron los *testing* que se debían llevar a cabo para probar el diseño y la efectividad de los controles y el alcance dentro del tiempo establecido, así como los recursos requeridos.

Una vez determinados estos pasos de prueba de las diferentes fases, se procede a la coordinación y realización de reuniones con la administración, a fin de validar el riesgo presentado, los controles establecidos y el alineamiento con las normativas internas vigentes, así como su cumplimiento.

Posterior a la ejecución de sesiones con los mandos medios, se procede a establecer visitas a las áreas con cada uno de los encargados de los controles en alcance, con el fin de realizar una indagación sobre su ejecución, fuentes de información, validaciones y procesos manuales que se realicen, así como reportería y evidencia generada a raíz de estas actividades. Finalmente, con la información recolectada se procedió a efectuar la prueba de diseño de los controles, cuyos resultados serán presentados en la etapa 3.

Seguidamente, para los controles con una conclusión de "Adecuado en diseño", se procedió a realizar la prueba de efectividad, tomando como población los ítems de julio a diciembre de 2017, de lo cual se obtuvieron resultados que serán presentados en la etapa 3 de la metodología de auditoría.

3.1.3 Etapa 3- Comunicación de resultados

A continuación se presenta el resumen del trabajo de auditoría realizado.

Control	Conclusión en diseño	Conclusión en efectividad
ITSOX014	Adecuado	Efectivo
ITSOX015	Adecuado	Inefectivo
ITSOX019	Adecuado	Inefectivo

Dichas conclusiones fueron presentadas a la organización, junto con recomendaciones para las efectuar mejoras que cada una requiere. Estas se abordan con más detalle en el capítulo 5 y 6 de este documento.

Sin embargo, por un requerimiento de confidencialidad acordado con la Empresa previo al inicio de este trabajo de investigación, y de acuerdo con lo establecido en los términos para su realización desde el inicio del curso Práctica Profesional I, no resulta factible incluir en este apartado la totalidad de la evidencia lograda. Esta fue entregada como parte del expediente entregado a las autoridades de la organización según consta en **ACT-AI-01** y fue expuesta a esas instancias según se indica en acta respectiva.

Se adjunta adicionalmente la carta de recibido conforme de la empresa sobre el trabajo realizado.

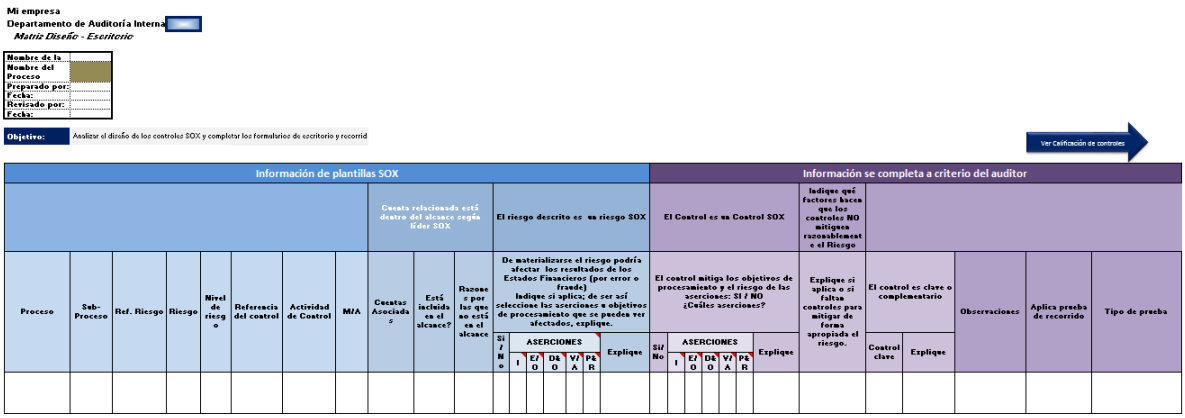
CAPÍTULO 4- MACHOTES DEL TRABAJO

Como parte del proceso de auditoría, fueron diseñados diferentes machotes de trabajo para cumplir con el objetivo y alcance de la misma. Estas se estructuraron de la siguiente manera:

Plantillas de revisión de diseño

Evaluación de escritorio

Plantilla Diseño- Escritorio


Mi empresa
Departamento de Auditoría Interna
Matriz Diseño - Escritorio

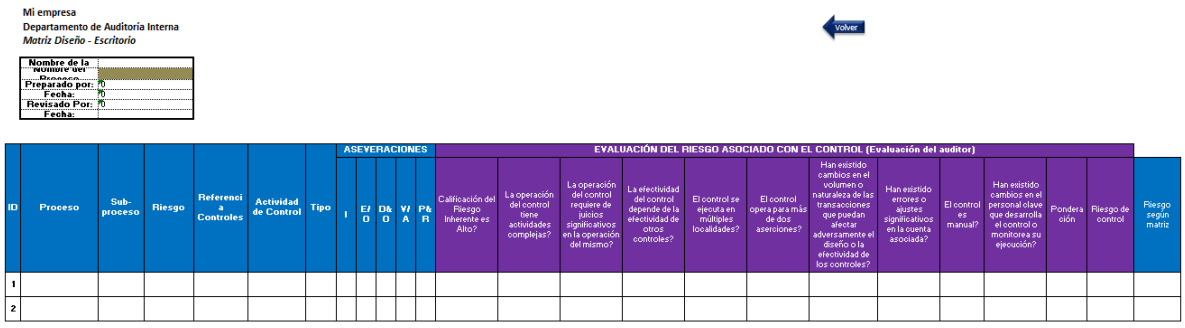
Nombre de la Nombre del Proceso
Preparado por:
Fecha:
Revisado por:
Fecha:

Objetivo: Analizar el diseño de los controles SOX y completar los formularios de escritorio y recorrid

Ver Calificación de controles

Información de plantillas SOX																						Información se completa a criterio del auditor																							
								Cuenta relacionada está dentro del alcance según líder SOX			El riesgo descrito es un riesgo SOX											El Control es un Control SOX								Indique qué factores hacen que los controles NO mitiguen razonablemente el Riesgo		El control es clave o complementario		Observaciones	Aplica prueba de recorrido	Tipo de prueba															
Proceso	Sub-Proceso	Ref. Riesgo	Riesgo	Nivel de riesgo	Referencia del control	Actividad de Control	M/A	Cuentas Asociadas	Está incluida en el alcance?	Razones por las que no está en el alcance	De materializarse el riesgo podría afectar los resultados de los Estados Financieros (por error o fraude) Indique si aplica; de ser así seleccione las aserciones u objetivos de procesamiento que se pueden ver afectados, explique.										El control mitiga los objetivos de procesamiento y el riesgo de las aserciones: SI / NO ¿Cuáles aserciones?								Explique si aplica o si falta controles para mitigar de forma apropiada el riesgo.	Control clave	Explique																	
											Si / No	ASERCIONES						Explique			Sí/ No	ASERCIONES						Explique																			
												I	E/O	D&O	V/A	P&R					I	E/O	D&O	V/A	P&R																					

Calificación de controles


Mi empresa
Departamento de Auditoría Interna
Matriz Diseño - Escritorio

Nombre de la Nombre del Proceso
Preparado por:
Fecha:
Revisado Por:
Fecha:

Volver

ID	Proceso	Sub-proceso	Riesgo	Referencia Controles	Actividad de Control	Tipo	ASEVERACIONES					EVALUACIÓN DEL RIESGO ASOCIADO CON EL CONTROL (Evaluación del auditor)												Ponderación	Riesgo de control	Riesgo según matriz
							I	E/O	D&O	V/A	P&R	Calificación del Riesgo Inherente es Alto?	La operación del control tiene actividades complejas?	La operación del control requiere de juicios significativos en la operación del mismo?	La efectividad del control depende de la efectividad de otros controles?	El control se ejecuta en múltiples localidades?	El control opera para más de dos aserciones?	Han existido cambios en el volumen o naturaleza de las transacciones que puedan afectar adversamente el diseño o la efectividad de los controles?	Han existido errores o ajustes significativos en la cuenta asociada?	El control es manual?	Han existido cambios en el personal clave que desarrolla el control o monitorea su ejecución?			
1																										
2																										

Evaluación de recorrido

Plantilla Diseño- Recorrido

Auditoría SOX | **Control**

Matriz SOX: **Periodo revisado:** **Fecha de revisión:** **Hecho por:**	
Fuente de información:	
Resultado:	
Conclusión:	
Notas aclaratorias	

Procedimiento de revisión (Testing)	

Link, revisión de riesgos asociados a	Ver revisión diseño del control vr riesgos asociados

Simbología de la revisión	
Cumple:	✓
No cumple:	✗
No aplica:	N/A
Énfasis en la revisión:	

Narrativa operativa del proceso control SOX #control

Participaron en la reunión del DD/MM/AA: Ver recorrido y documentación reporte

Comunicación de resultados

Revisión de riesgos asociados al control - Revisión de diseño

Revisión de riesgos asociados al control - Revisión de diseño							
Información tomada de la declaración de controles SOX						Revisión de auditoría	
Proceso	Sub-proceso	Referencia Riesgos	Riesgo	Referencia Controles	Actividad de Control	Actividad mitiga el riesgo	Justifique en caso de no mitigar

Documentación soporte del recorrido

Documentación soporte del recorrido

Plantilla de revisión de efectividad

Plantilla de información de muestra

Auditoría SOX

Referencia control SOX	
Proceso del control SOX	
Realizado por	
Criterio de selección de la muestra	

Información del tamaño de la muestra

Según lo establecido en la siguiente tabla:

Frecuencia del Control	Población asumida Ocurrencias Control	Número de muestras a probar	
		Bajo	Alto
Anual			
Semestral			
Trimestral			
Mensual			
Quincenal			
Semanal			
Diario			
Multiples veces al día			

Nivel de riesgo	
Frecuencia	
Tamaño de muestra	#N/A

Seleccione el "Nivel de riesgo" y la "Frecuencia" según el control a evaluar

Información sobre la muestra / población

Tamaño muestra total	#N/A
Tamaño de la población	
Periodo de revisión	
Cantidad de elementos de la muestra a probar	
Porcentaje probado	#N/A

Histórico de evaluación de la muestra para el año en curso

	Fase
Cantidad de elementos probados de la muestra	0
Porcentaje probado sobre el total de la muestra	#N/A
Total de elementos probados durante el año	0
Tamaño de la muestra a evaluar en el año	#N/A
Diferencia entre el total de la muestra a probar y los elementos probados	#N/A

Plantilla de selección de la muestra

Auditoría SOX

Referencia control SOX	#¡VALOR!
Proceso del control SOX	#¡VALOR!
Realizado por	
Fuente de la información (¿De donde se obtiene la población?)	
Notas aclaratorias	

Selección de la muestra	
Población original	
Evidencia extracción del Query (si aplica)	

Prints del aplicativo con la evidencia de la obtención de la muestra aleatoría

Detalle de la muestra aleatoría seleccionada

Print de pantalla

Plantilla resumen de efectividad

Auditoría SOX

Referencia control SOX	
Proceso del control SOX	
Realizado por	
Fuente de información	
Naturaleza de la prueba	Inspección - Examinación
Notas aclaratorias	

Análisis de riesgos	Referencia
Ir a evidencia del análisis de riesgos	Ir

Testing a evaluar	Atributo/ Link
Paso 1	1
Paso 2	2
Paso 3	3
Paso 2	4

Según el tipo de prueba se debe de realizar un paso por cada pestaña de excel (ejem. PT1), para lo cual podemos realizar el link directamente del paso al PT1.

Resultado de la revisión:

Marcas de revisión	✓	Satisfactorio	✗	Insatisfactorio	n/a	No aplica

Datos de la muestra							Atributos				
Operación	DETALLE	CUENTA CONTABLE	FECHA VALOR	DETALLE	MONED.	Monto	1	2	3	4	Link
											PT1

Conclusión de la prueba

Oportunidades de mejora (si aplica):	Evidencia (Correo)

Análisis de riesgos de efectividad

Auditoría SOX
Análisis del Riesgo asociado al control

Referencia control SOX	0
Proceso del control SOX	0
Realizado por	0
Notas aclaratorias	

Volver

Análisis del control:

Actividad de Control	Sub-Proceso	Ref. riesgo	Riesgos asociados	¿El control mitiga el riesgo? ¿En cuales aserciones?						¿Es control clave?	¿El riesgo esta cubierto por otros controles?		Comentarios del Análisis Riesgo/Control	Comentarios del Análisis Productos
				Si/No	ASERCIONES						Si/No	¿Cuales?		
					I	E/O	D&O	V/A	P&R					

Evidencia de duplicados en la matriz:
(Pegar el print del asocie de los controles duplicados)

Paso de prueba

Auditoría SOX

Volver

Paso del testing a evaluar o atributo	Resultado

1. Evidencia de la revisión realizada para la valoración del paso del testing

CAPÍTULO 5- RESULTADOS

Posterior a la ejecución de cada una de las fases de prueba de controles en alcance, se obtienen los siguientes resultados:

Control ITSOX014 – Accesos a los sistemas de información

Prueba de diseño

El resultado de la revisión de diseño del control SOX ITSOX014 es adecuado, ya que se revisó la muestra de ítems y se concluye que son aprobadas por un nivel superior, y en el caso de las solicitudes de usuarios de bases de datos o sistema operativo son atendidas por Seguridad de Sistemas u Operaciones según corresponda.

Prueba de efectividad

Al finalizar con la revisión del control ITSOX014, con corte a diciembre de 2017, se concluye el control como Efectivo, debido a que la totalidad de solicitudes de Usuarios Especiales AD o Local fueron atendidas según se describe en la declaración.

Esto de acuerdo con las pruebas establecidas según lo indicado en la redacción del control, aplicadas a una muestra de solicitudes de creación o modificación de accesos para sistemas en alcance SOX y solicitud de usuarios de Base de datos o de AD o local. Esta situación mitiga de forma razonable el riesgo de pérdida de integridad de información utilizada para la generación de los estados financieros, por accesos no autorizados o inadecuada segregación de funciones en las aplicaciones, bases de datos o sistemas operativos bajo alcance SOX.

Control ITSOX015 – Cambios a parámetros de seguridad

Prueba de diseño

El resultado de la revisión de diseño del control SOX ITSOX015 es adecuado, ya que se revisó la población de cambios en parámetros de seguridad para las plataformas en alcance y se concluye que son alertados por las herramientas de monitoreo. Entre ellas está el ingreso de una boleta de Service Desk por el encargado de seguridad, que permite obtener la justificación respectiva del caso.

Por tanto, mitiga el riesgo para el cual está diseñado y se ejecuta tal cual indica la matriz SOX V008.

Prueba de efectividad

Al finalizar la revisión del control ITSOX015 con corte a diciembre de 2017, se concluye el control como Inefectivo, debido a que de un total de 10 alertas de cambios de parámetros de seguridad recibidas en el período, se identifican las siguientes deficiencias en la ejecución del control:

1- Se identifica una alerta el 31 de octubre de 2017 para la cual no se ingresó la boleta de investigación de Service Desk requerida, por consiguiente no se ejecutó el control.

La situación anterior expone al Grupo a un riesgo de pérdida de integridad de la información utilizada para la generación de los estados financieros debido a la puesta en producción de aplicaciones nuevas o errores en versiones en programas, cambios en las existentes o cambios en las bases de datos, sin ejecutar pruebas de manera no autorizada.

Se reitera que las causas para concluir el control como inefectivo son:

-No ejecución del control para una alerta.

Control ITSOX019 – Pruebas de restauración de cintas de respaldo

Prueba de diseño

El resultado de la revisión de diseño del control SOX ITSOX019 es adecuado, ya que se revisó la población de pruebas de respaldo de cintas para las plataformas en alcance y se concluyó que son ejecutadas oportunamente, con personal idóneo para ello y aprobadas por la administración.

Por tanto, lo anterior mitiga el riesgo para el cual está diseñado y se ejecuta tal cual indica en la matriz SOX V008.

Prueba de efectividad

Al finalizar con la revisión del control ITSOX019 con corte a diciembre de 2017, se concluye el control como Inefectivo, debido a que de un total de 7 pruebas de restauración programadas en el período, se identifican la siguiente deficiencia en la ejecución del control:

1- Se identifica que la prueba programada para el día 11 de setiembre de 2017 referente a la plataforma SYSTEM no fue ejecutada.

La situación anterior expone al Grupo a un riesgo de "Pérdida de integridad de la información utilizada para la generación de los estados financieros, por fallas en el proceso de recuperación de datos y aplicaciones alcanzadas SOX".

Se reitera que las causas para concluir el control como inefectivo son:

-No ejecución de una prueba de restauración.

CAPÍTULO 6- CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones del estudio aplicado y sus recomendaciones

Como parte del estudio realizado, se obtienen las siguientes recomendaciones u oportunidades de mejora en la ejecución y diseño de los controles.

Control ITSOX014 – Accesos a los sistemas de información

Se identifican las siguientes oportunidades de mejora en la definición y ejecución del control:

1- Incluir un control mitigante para las solicitudes de acceso que no son procesadas automáticamente, para verificar que el usuario creado se alinea a la solicitud aprobada por el nivel superior respectivo.

2- Incluir dentro del control la creación y modificación de accesos para *outsourcing*.

3- Actualizar el control de la matriz actual para que incluya la herramienta de gestión de salidas y movimientos, la cual desde octubre tramita la creación de usuarios de red.

4- Se recomienda separar en un control la gestión de solicitudes de acceso y en otro control la gestión de solicitudes a bases de datos y sistemas operativos, debido a que al ser poblaciones gestionadas de forma diferente, no pueden tomarse como parte de un mismo control.

5- Se recomienda definir qué es un nivel superior y la estructura organizativa de puestos en la cual basarse para este fin, así como generar documentación de las excepciones que puedan existir en el flujo.

6- Dos solicitudes presentan conflictos de segregación de funciones ya que los aprobadores de las diferentes partes (Supervisor, seguridad y Operaciones TI) se repiten e inclusive en un caso coinciden con las de el que ingresa la solicitud, por lo que se recomienda garantizar que la tríada de aprobadores se conforme por personas diferentes.

7- Las solicitudes de usuarios de Base de datos o de AD o local deben reflejar en la boleta de atención de *service desk* la consistencia con la categoría asignada en la boleta de solicitud de

usuarios de Base de datos o de AD o local. Se recomienda verificar en las revisiones realizadas por la tríada de aprobadores que realmente corresponda al tipo de solicitud que se está ingresando.

8- Se recomienda definir oficialmente la lista de servidores y bases de datos a los cuales les aplica el control, así como las excepciones que se puedan generar en la atención de la boleta, producto de la misma operativa. Asimismo, se debe definir un mecanismo para identificar apropiadamente las solicitudes de usuarios de Base de datos o de AD o local con la plataforma que afecta y obtener la población total del período.

Control ITSOX015 – Cambios a parámetros de seguridad

Se identifican las siguientes oportunidades de mejora en la ejecución del control:

1-Se identifica una alerta para la cual en la boleta de Service Desk no se adjunta una justificación oficial (Plan de Trabajo, Solicitud de cambio, boleta o incidente): para ello se recomienda garantizar que cada boleta de investigación cuente con una justificación válida y modificar el manual operativo.

Control ITSOX019 – Pruebas de restauración de cintas de respaldo

Se identifican las siguientes oportunidades de mejora en la ejecución del control:

1-Se identifica que el cronograma de pruebas de restauración no se encuentra actualizado, lo cual provoca que las fechas de realización de las pruebas y la fecha del cronograma no coincidan. Para ello se recomienda mantener un calendario actualizado con las debidas reprogramaciones que se aprueben durante el año, con el objetivo de poder mantener un adecuado control sobre lo pendiente y una homogeneidad entre los insumos del control.

6.2 Conclusiones del proyecto realizado

Como parte de la experiencia al realizar este proyecto se obtienen las siguientes conclusiones:

1. Es muy importante mantener una fuente independiente que pueda garantizar la integridad de los datos durante la extracción de información y la obtención de los insumos.

2. El integrarse a un proyecto de cumplimiento regulatorio tan importante para una organización permite alinear esfuerzos con la administración para salvaguardar los intereses de los accionistas y conocer el esquema de control interno que rige dentro de una empresa, así como evaluar su robustez.
3. La definición del *testing* de los controles es la actividad crucial en una auditoría SOX, debido a que este nos guiará en el transcurso del análisis de información y permitirá identificar vulnerabilidades de diseño o incumplimientos con su ejecución, así como agregar valor mediante oportunidades de mejora.
4. Previo al inicio de las fases de diseño y efectividad, es prioritario obtener un conocimiento del riesgo que mitiga el control, así como de la operativa del área y los sistemas y el flujo de información que se procesa.

6.3 Recomendaciones generales

1. Se recomienda establecer cuál es el valor agregado de cada proyecto de auditoría previo a su inicio y analizar su alineación con las expectativas y estrategias del negocio.
2. Es importante tomar en cuenta, al establecer las recomendaciones, la opinión de la administración y el impacto en la operativa y administración del mismo, siempre orientado a optimizar costos y recursos.

Bibliografía

Barrantes, R. (1999). *Investigación. Un camino al conocimiento: Un Enfoque Cuantitativo y Cualitativo.* San José, Costa Rica: EUNED.

Barrantes, E. R. (2009). *La investigación: un camino al conocimiento*. San José, Costa Rica: UNED. Recuperado el 17 de octubre del 2017, de https://www.uned.ac.cr/academica/images/ceced/docs/Investigacion_camino_conocimiento.pdf, a las 15 horas.

CGR. (2014). *Normas Generales de Auditoría para el Sector Público*. San José: Contraloría General de la República de Costa Rica. Recuperado el 30 de 09 de 2017, de www.cgr.go.cr

Auditoría Interna. (2016). *Manual Operativo Pruebas de efectividad SOX*. San José, Costa Rica.