GUÍA DE AUDITORÍA PARA LA EVALUACIÓN DEL CONTROL INTERNO DE TI EN LAS ENTIDADES PÚBLICAS

Diana Tinoco[1], Francisco Aguirre[2], Vicente Merchán[3]

[1,2,3] Departamento de Ciencias de la Computación; Universidad de las Fuerzas Armadas, Sangolquí, Ecuador.
diana2_us@yahoo.com;desafiopersonal@yahoo.com;
vrmerchan@espe.edu.ec

Resumen: El presente artículo tiene como objetivo mostrar el desarrollo de la Guía de Auditoría para la Evaluación del Control Interno en el área de TI en las Entidades Públicas del Ecuador, para el cual se realizó el análisis de la base legal ecuatoriana de cumplimiento obligatorio en las entidades públicas, identificación de las áreas a analizar, evaluación de riesgos, controles claves, procedimientos de auditoría y el proceso de la auditoría. Además se realizó la aplicación práctica de la guía en la que se efectuó, el diagnóstico preliminar, la aplicación de cuestionarios de control interno, evaluación de riesgos y los comentarios de control interno

Palabras Clave: Control interno, Tecnologías de Información, riesgos, auditoría.

Abstract: This article aims to show the development of the Audit Guide for the evaluation of internal control in the area of IT in public entities of Ecuador, therefore was fundamental the analysis of Ecuadorian laws binding in public sector, identifying areas to analyze, evaluate risks, key controls, audit procedures and the audit process. Besides the practical application of the guide consist in: preliminary diagnosis, implementation of internal control questionnaires, risk assessment and internal control comments.

Keywords: Internal control, Information Technology, risks, audit.

I. INTRODUCCIÓN

El control interno Informático controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo con los procedimientos y estándares fijados por la Unidad de Tecnología, así como los requerimientos legales de la entidad, normas de control interno y requerimientos legales para la administración pública.

De la revisión a los informes aprobados en el año 2012 por la Contraloría General del Estado, se observa que existen entidades públicas que no han implementado controles en los procesos y servicios de Tecnologías de Información como: Seguridades de tecnologías de información, controles de aplicación, políticas procedimientos y estándares entre otras, lo que no ha permitido que se pueda brindar una seguridad razonable del logro de la misión y objetivos institucionales.

Es por ello que se propuso el desarrollo de una Guía de Auditoría para la Evaluación del Control Interno en el área de TI en las Entidades Públicas del Ecuador que permite evaluar el control interno de TI, de acuerdo a la normativa existente y actualizada, que permita determinar su nivel de fortaleza, estableciendo si existe una seguridad razonable o poco confiable de las operaciones y procesos sistematizados,

ayudando a que todos los miembros de la empresa que operan los sistemas informáticos sean partícipes de sus deberes y responsabilidades, de manera que su accionar sea el más adecuado para el cumplimiento de los objetivos organizacionales.

II. METODOLOGÍA.

Los métodos teóricos utilizadas son las siguientes: analítico utilizado en la etapa inicial para separar el control interno informático en partes bien diferenciadas, sintético empleado en cada una de las áreas de la tecnología de información y deductivo para analizar las diferentes metodologías que son aplicadas para la evaluación del control interno de TI.

La metodología utilizada de análisis de riesgos con la finalidad de identificación de la falta de controles y el establecimiento de un plan de contramedidas. En base a unos cuestionarios, se identifican vulnerabilidades y riesgos, y se evalúa el impacto para más tarde identificar las contramedidas y llegar al informe final.

El auditor debe evaluar y supervisar los controles de TIC que son parte integral del entorno de control interno de la organización, proponiendo al Área de Tecnología de Información y Comunicaciones consejos con respecto al diseño, implementación, operación y mejora de controles de TIC. (Iglesias & Monterrosa, 2011)

Es importante definir algunos conceptos y definiciones como:

a) **Proceso de la auditoría para las entidades públicas.** (Contraloría General del Estado, 2013)

Orden de Trabajo.- Los Directores de las Unidades de Control emite la orden de trabajo, documento que determina: el tipo y nombre de la acción de control, la institución responsable de la ejecución o manejo del proyecto, las instituciones relacionadas, el alcance, el periodo a hacer examinado, los objetivos, la conformación del equipo de trabajo, la distribución de las responsabilidades y el tiempo asignado.

Notificación de Inicio.- De manera simultánea a la emisión de la orden de trabajo, el Director de la Unidad de Control o Delegado Provincial pertinente comunica el inicio de la acción de control a la máxima autoridad de la entidad auditada, incluyendo los contenidos establecidos en el artículo 20 del Reglamento a la Ley Orgánica de la Contraloría General del Estado.

Solicitud inicial de información.- Luego de la emisión de la orden de trabajo y las notificaciones de inicio a las máximas autoridades de la entidad auditada y de las instituciones relacionadas, se emite las solicitudes iniciales de información con la finalidad de recopilar información básica que permita al auditor conocer a la entidad a ser auditada, elaboradas por el jefe de equipo de acuerdo a los artículos 76 y 88 de la Ley Orgánica de la Contraloría General del Estado y 7 de su Reglamento de aplicación.

Diagnóstico general y planificación.- A más de la documentación de la información recibida y recopilada, es necesario realizar reuniones de trabajo con las personas vinculadas con la auditoría, y de ser el caso inspecciones de campo a las instalaciones de la entidad, a las diferentes áreas a evaluar.

Desarrollo y recopilación de información.- En esta etapa comprende el desarrollo de los cuestionarios de control interno y la evaluación de riesgos con la finalidad de

identificar las áreas críticas aplicar los procedimientos de auditoría, y si es necesario solicitar información como evidencia de los hallazgos realizados.

Comentarios, conclusiones y recomendaciones.- Los comentarios consisten en la exposición de condición, criterio, causa y efecto de los hallazgos obtenidos en la ejecución de la acción de control.

Las conclusiones representan los pronunciamientos profesionales del auditor sobre el análisis del control interno, se sustentan en el análisis de la evidencia de la auditoría, identificando los responsables de las inobservancias de carácter técnico, legal o económico, describiendo la norma que inobservó y las consecuencias y efectos para la institución. Y las recomendaciones son las acciones que se requiere para corregir los incumplimientos detectados.

Comunicación de resultados e informe final.- En cumplimiento a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, los auditores en el desarrollo de la acción de control deben mantener la comunicación con los servidores de la organización auditada y demás personas relacionadas con las actividades relacionadas.

La comunicación de resultados provisionales, se realizará al finalizar el trabajo de campo mediante un documento escrito en el que se incluirá los comentarios y conclusiones referentes a los hallazgos significativos detectados.

No se incluirán las recomendaciones con la finalidad de cumplir con el debido proceso y dar oportunidad a los auditados de presentar documentos que aclaren o desvirtúen los hallazgos.

Seguimiento.- Una vez receptado el informe final aprobado por la Contraloría General del Estado, las entidades auditadas, deberán elaborar un plan que permita aplicar las recomendaciones emitidas, en el cual se determinará las actividades necesarias como: recursos, responsables y tiempos. La Contraloría General del Estado puedo evaluar, la efectividad de las recomendaciones emitidas a través del seguimiento.

b) Base Legal

Para efectuar la evaluación de control interno informático es necesario tomar en cuenta la siguiente base legal. (Constitución de la República del Ecuador, 2008) (Código Orgánico de Planificación y Finanzas Públicas, 2010) (Ley Orgánica de la Contraloría General del Estado, 2002) (Ley del Sistema Nacional de Registro de Datos Públicos, 2010) (Ley Orgánica de Transparencia y Acceso a la Información Pública, 2004) (Ley de Comercio Electrónico, Mensaje de Datos y Firmas Digitales., 2002) (Ley Orgánica del Sistema Nacional de Contratación Pública, 2008) (Ley Orgánica de Transparencia y Acceso a la Información Pública, 2004) (Reglamento General a la Ley Orgánica de Transparencia y Acceso a la Información Pública y Reformas, 2005) (Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública, 2009) (Contraloria General del Estado, 2006) (Normas de Control Interno, 2009)

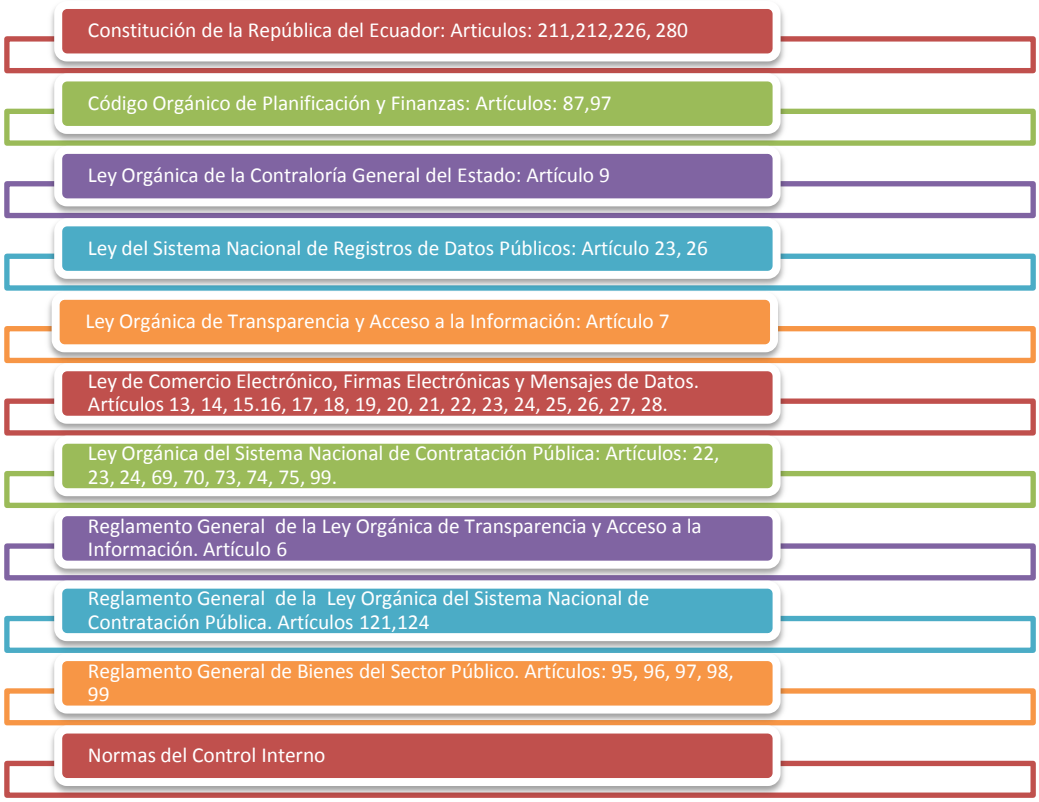

Figura 1. Base Legal

Mejores Prácticas.

COBIT (Objetivos de Control para las Tecnologías de Información): Es una herramienta de gobierno de TI, que vincula las tecnologías informáticas y prácticas de control agrupadas en cinco dominios. (ISACA, 2012)

ITIL (Information Technology Infraestructure Library) es una colección de las mejores prácticas observadas en la industria de TI. Es un conjunto de libros en los cuales se encuentran documentados todos los procesos referentes a la provisión de servicios de tecnología de información hacia las organizaciones.

Norma ISO 27000 Es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información, su objetivo es proporcionar una base común para desarrollar normas de seguridad dentro de la organización.

III. EVALUACIÓN DE RESULTADOS Y DISCUSIÓN

1. Áreas a evaluar.

De acuerdo al análisis de la estructura organizacional de la Unidad de Tecnología diferentes entidades públicas y de acuerdo a las Normas de Control Interno se identificaron las siguientes áreas e identificamos los medios de verificación para su cumplimiento

Figura 2.- Áreas a Evaluar

- **Organización y administración:**
  - Estructura Organizacional
    - Organigrama de la Unidad de Tecnología de Información y Comunicación.
    - Orgánico funcional aprobado.
  - Segregación de Funciones
    - Descripción documentada y aprobada de los puestos de trabajo.
    - Resultados de la evaluación de desempeño.
  - Plan Informático Estratégico y Tecnología
    - El Plan estratégico y operativo de tecnología de información y su presupuesto analizados y aprobados por la máxima autoridad de la entidad y que al menos incluya:
  - Políticas y Procedimientos.
    - Políticas y procedimientos aprobados por la máxima autoridad y difundidos
  - Modelo de Información Organizacional
    - Diccionario de datos, Modelo entidad – relación, Modelo físico.
  - Proyectos Tecnológicos
    - Documentos entregables con sus respectivas aprobaciones, documentos formales como actas o documentos electrónicos legalizados.
    - Plan de control de cambios aprobado
    - Plan de aseguramiento de la calidad aprobado
  - Capacitación.
    - Plan de capacitación informático, formulado conjuntamente con la unidad de talento humano.
  - Comité Informático.

        - Resolución de la entidad en donde se encuentre: creación y objetivos, integración, funciones, sesiones, subcomisiones de apoyo

- **Sistemas Informáticos**
    - Políticas de Software
        - Políticas y estándares de software aprobados y difundidos.
        - Metodologías y procedimientos definidos en el desarrollo de software.
    - Adquisición de Software
        - Plan Anual de Compras de la Institución, Portafolio de proyectos, Documento que se solicita el requerimiento, la necesidad, Pliegos, Contrato, Actas entrega-recepción.
        - Procedimiento precontractual, contractual y ejecución que se realiza en el Sistema Nacional de Compras Públicas.
    - Desarrollo de Software
        - Portafolio de proyectos y servicios.
        - Requerimientos funcionales y técnicos
        - Actas de aceptación por parte de los usuarios.
        - Manuales técnicos, instalación, configuración, y de usuario
    - Mantenimiento de Software.
        - Procedimientos para el mantenimiento y liberación del software de aplicación.
        - Registro del control de cambios.
        - Registro de control de versiones.
        - Manuales técnicos y de usuarios actualizados.
        - Verificar si existe ambientes de desarrollo, prueba y producción.
        - Diagramas y configuraciones de hardware y software
    - Aplicaciones y Servicios
        - Instructivos de instalación, configuración y uso de los servicios de intranet, internet y correo electrónico.
- **Infraestructura Tecnológica**
    - Administración de la Infraestructura
    - Adquisición de Infraestructura
        - Plan Anual de Compras de la Institución, Portafolio de proyectos, Documento que se solicita el requerimiento, la necesidad, Pliegos, Contrato, Actas entrega-recepción.
        - Los mismos procedimientos precontractuales y contractuales aplicados por el Sistema Nacional de Compras Públicas.
        - Determinar la correspondencia de las características técnicas entre los equipos adquiridos, especificaciones técnicos y requerimientos establecidos en las fases precontractual, contractual y confirmado en las actas entregas recepción.
    - Mantenimiento y Soporte de la Infraestructura.
        - Políticas y procedimientos emitidos para el mantenimiento de la infraestructura tecnológica.
        - Plan de mantenimiento preventivo y correctivo de la infraestructura tecnológica.

- **Seguridades**
    - Políticas y procedimientos aprobados y difundidos para proteger y salvaguardar los bienes y la información.
    - Constatación física de la ubicación e instalaciones físicas de la Unidad de Tecnología de Información y del Centro de Datos.
    - Políticas y procedimientos para la obtención de respaldos.
    - Plan de Contingencia aprobado e implementado

- **Monitoreo y Evaluación**
    - Procesos y Servicios
        - Indicadores de desempeño definidos
        - Medidas o procedimientos definidos para el análisis de satisfacción al cliente
        - Informes de gestión
        - Metodologías utilizadas para la evaluación y monitoreo

2. Evaluación de riesgos

La evaluación de riesgos comprende su identificación, análisis, mapeo, priorización y tratamiento. (ISO. International Organization for Standarization, 2009)

- **Identificación del Riesgo**.- Se realizó la identificación de riesgos de acuerdo a las áreas, se identificó el objetivo, las fuentes de riesgo, las causas y las consecuencias potenciales.
- **Análisis del Riesgo.-** Con los riesgos identificados se identificó los controles existentes, se definió la efectividad de los controles, para luego definir la probabilidad de ocurrencia y el impacto de los riesgos.
- **Mapeo de Riesgos.-** una vez definido la probabilidad y el impacto se procede a ubicarlos en el mapa de riesgos.
- **Priorización de los Riesgos.-** Que ayudan a identificar la prioridad para su tratamiento
- **Tratamiento de los Riesgos.-** El tratamiento de los riesgos involucra seleccionar una o más acciones para implementarlas y mitigar los riesgos identificados, estas pueden ser: evitar, reducir, compartir y aceptar el riesgo. Se definió un indicador de desempeño para la administración de riesgos, por cada acción propuesta.

  El resultado de la evaluación de riesgos es la siguiente:

RIESGOS	Probabilidad	Impacto	Nivel de riesgo	Priorización	Acciones propuestas
1. La falla de componentes que conforman el centro de datos, el acceso no autorizado a los equipos y a la información, el ingreso de personas no autorizadas al Data Center, falta de ambientes de desarrollo, prueba y producción y de almacenamiento, el mal uso de los servicio por parte de los usuarios y la falta de procedimientos definidos PODRIAN OCASIONAR que no se garantice que los servicios estén disponibles, seguros y confiables para el usuario final.	3	3	15	3	Reducir
2. La falta de recursos de la infraestructura en los servidores, que el personal que utiliza los sistemas no esté capacitado, el no poder dar soluciones de mantenimiento, ni realizar actualizaciones a los sistemas PODRIAN OCASIONAR que no se mantengan las aplicaciones institucionales operativas y actualizadas.	4	3	12	2	Reducir
3. La falta de involucramiento de las unidades requirientes, alta rotación del personal, falta de formalidad en el manejo de los procesos y metodologías de trabajo y la no disponibilidad de equipamiento tecnológico suficiente PODRIA OCASIONAR que las aplicaciones desarrolladas no cumplan con la funcionalidad requerida por los clientes internos.	4	4	16	1	Compartir
4. La falta de involucramiento de las unidades requirientes, alta rotación del personal, falta de formalidad en el manejo de los procesos y metodologías de trabajo suficiente PODRIA OCASIONAR que las aplicaciones desarrolladas no cumplan con la funcionalidad requerida por los clientes internos.	4	5	20	5	Reducir
5. La alta rotación del personal, alta depreciación y caducidad del soporte y mantenimiento de la infraestructura tecnológica y que los proyectos elaborados no puedan tener su curso normal para su ejecución, PODRIAN OCASIONAR que no se planifique y administre adecuadamente los recursos tecnológicos de la institución.	4	4	16	4	Reducir

Tabla 1. Riesgos

IV. TRABAJOS RELACIONADOS.

Este documento contiene la información necesaria para poder realizar la evaluación de control interno informático de TI de las entidades públicas del Ecuador, q por ser evaluada en base a la legislación ecuatoriana no se encuentran trabajos similares en este aspecto. El control interno informático es universal por lo que existen controles claves, procedimientos de auditoria a ser aplicados en las diferentes áreas, similares a los que se presenta en esta guía, sin embargo el trabajo sustenta la base legal para evaluar estos controles.

Existen otros trabajos como Manual de Auditoría de Gestión a las Tecnologías de Información y Comunicaciones de la Corte de Cuentas de la República del Salvador, (Iglesias & Monterrosa, 2011) en la que los auditores sustentan su trabajo en conclusiones basadas en indicadores de gestión del área de tecnologías de Información y Comunicaciones; y que como parte de esta auditoria se evalúa el control interno, por eso es importante indicar que aunque se presenten evaluaciones de controles informáticos similares el propósito de las auditorias son diferentes.

V. CONCLUSIONES Y TRABAJO FUTURO.

De acuerdo a las encuestas realizadas se concluye que existe un gran desconocimiento de las normas de control interno por parte de los servidores públicos, que hace que no estén familiarizados con los controles que deben implementar, sin embargo está vigente el principio jurídico que dice el desconocimiento de la ley no justifica la culpa.

El 87% de las instituciones públicas encuestadas indicaron que no tienen definidos los procesos del TI, es por ello que para el diseño de la presente guía de auditoría se efectuó por áreas.

No existen controles permanentes, ya que de acuerdo a la encuesta realizada el 86% de las instituciones públicas indicaron que no se realizan evaluaciones de control interno en el área de TI.

De la aplicación de la metodología de riesgos se obtuvo que las áreas con mayor nivel de riesgos son: la de organización y administración, seguida por la administración de servidores, redes y comunicaciones y la de soporte a usuarios y mantenimiento a equipos.

Se desarrolló e implementó cuestionarios de control interno para cada área de TI, incluyendo preguntas de acuerdo a las Normas de Control Interno para las entidades públicas.

Los medios de verificación o controles identificados en las diferentes áreas, ayudan en el proceso de solicitud de información, que de no ser presentados, sirven de evidencia por incumplimiento de los mismos.

Se recomienda, socializar los contenidos de las legislaciones pertinentes con la finalidad que se den cumplimiento, aplicar los cuestionarios de control interno de acuerdo a la estructura organizacional de la institución, que en las instituciones públicas se haga el levantamiento de procesos del área de TI, realizar evaluaciones periódicas de control interno con la finalidad de evitar riesgos y tener una mejora continua en los procesos, que en la fase de evaluación de riesgos, se realicen reuniones de trabajo con las diferentes áreas con la finalidad de conocer las deficiencias que presenta cada una de ellas, además de realizar el monitoreo y seguimiento a las observaciones realizadas.

REFERENCIAS BIBLIOGRÁFICAS

Constitución de la República del Ecuador. (2008). Registro oficial 449 del 20 de octubre del 2008.

Código Orgánico de Planificación y Finanzas Públicas. (2010). Registro Oficial 306 del 22 de octubre del 2010.

Contraloria General del Estado. (2006). *Reglamento General de Bienes del Sector Público*. Registro oficial 378 del 17 de octubre del 2006.

Contraloría General del Estado. (25 de 09 de 2013). *Guía de Auditoría Ambiental*. Recuperado el 10 de 10 de 2013, de CGE: http://www.contraloria.gob.ec/normatividad_vigente.asp

Iglesias, C. E., & Monterrosa, J. S. (10 de 2011). *Manual de Auditoria de Gestión de Tecnologías de Información*. Recuperado el 01 de 07 de 2013, de sitio web de OLACEFS: http://http://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCgQFjAA&url=http%3A%2F%2Fbibliotecavirtual.olacefs.com%2Fgsdl%2Fcollect%2Fguasyman%2Farchives%2FHASH0155.dir%2FManualAuditoriaGestionTICs.pdf&ei=oDU8U8rsB-vgsATtyIKYDg&usg=AFQj

ISACA. (2012). *The Cobit Framework*. Recuperado el 02 de 08 de 2013, de ISACA: http://isaca.org/Content/NavagationMenu/Members_and_Leaders/COBIT6/Obtain_COBIT/Cobit4_Español.pdf

ISO. International Organization for Standarization. (2009). *31000*.

Ley de Comercio Electrónico, Mensaje de Datos y Firmas Digitales. (2002). Registro Oficial 557 del 17 de abril del 2002.

Ley Orgánica de la Contraloría General del Estado. (2002). Registro Oficial 595 del 16 de junio del 2002.

Ley Orgánica de Transparencia y Acceso a la Información Pública. (2004). Registro oficial 337 del 18 de mayo del 2004.

Ley Orgánica de Transparencia y Acceso a la Información Pública. (2004). Registro oficial 337 del 18 de mayo del 2004.

Ley Orgánica del Sistema Nacional de Contratación Pública. (2008). Registro oficial 395 del 4 de agosto del 2008.

Ley del Sistema Nacional de Registro de Datos Públicos. (2010). Resgistro oficial 162, 31 de marzo del 2010.

Normas de Control Interno. (2009). Acuerdo 039 CG.

Reglamento General a la Ley Orgánica de Transparencia y Acceso a la Información Pública y Reformas. (2005). Registro oficial 507 del 19 de enero del 2005.

Reglamento General a la Ley Orgánica del Sistema Nacional de Contratación Pública. (2009). Registro Oficial 588 del 8 de mayo del 2009.