

# ● AUDITORÍA A LA GESTIÓN DE LAS TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

## RESUMEN

El artículo plantea utilizar la Auditoría Informática como una herramienta que gestione el uso adecuado de la tecnología de información, apoyado en la aplicación de la normativa legal y en estándares informáticos internacionales. En la metodología se han considerado dos aspectos básicos: La identificación de áreas de riesgo y la identificación de áreas de control.

**Palabras Claves:** Auditoría informática. Riesgos informáticos. Tecnología de la información.

## ABSTRACT

This article outlines the use of computing audit as a tool to exert a suitable use of information technology, supported by applying legal regulations as well as international computing standards. In methodology, two basic features have been considered: both risk areas and control areas identification.

**Key Words:** Computing audit. Computing risks. Information technology.

<sup>(1)</sup> Guadalupe Ramírez R.

<sup>(2)</sup> Ezzard Álvarez D.

## INTRODUCCIÓN

Una de las principales preocupaciones de las Entidades Públicas que han realizado ingentes esfuerzos en la implementación de tecnologías de información, es que probablemente no ven que las inversiones que han realizado den soluciones inmediatas, tangibles y medibles; y allí donde se veía una oportunidad de mejora, realmente están creando un problema difícil de administrar, controlar y caro de mantener. La Auditoría Informática se constituye en una herramienta que gestiona la tecnología de la información en las entidades, a través de auditorías internas y externas.

El presente trabajo propone una metodología de auditoría informática con la finalidad de medir los riesgos y evaluar los controles en el uso de las tecnologías de información, haciendo uso de técnicas y estrategias de análisis, que permitan que la auditoría informática se convierta en una real y eficiente herramienta de gestión de tecnologías de información, a disposición de las Entidades Públicas.

## COMPENDIO DE NORMATIVIDAD SOBRE EL USO DE TECNOLOGÍAS DE INFORMACIÓN EN EL PERÚ

El Instituto Nacional de Estadística e Informática del Perú ha publicado su obra titulada "Compendio de Normatividad sobre el uso de Tecnologías de Información en el Perú", la misma que compila la legislación establecida por el Gobierno y el Congreso de la República. Se inicia con los mandatos previstos en la Constitución de Política, continúa con las leyes que garantizan la libertad de información, leyes de derecho de autor y derechos conexos, normas sobre delitos informáticos, normas sobre firmas y certificados digitales, la ley que permite la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad, normas sobre el uso de Tecnologías de Información en la gestión de archivos y documentos y normas que regulan el uso de formatos electrónicos en las instituciones de Administración Pública.

## NORMAS TÉCNICAS DE CONTROL INTERNO PARA EL SECTOR PÚBLICO

Las Normas de Control Interno para el Sector Público son guías generales dictadas por la Contraloría General de la República, con el objeto de promover una sana administración de los recursos públicos en las entidades en el marco de una adecuada estructura del control interno. Estas normas establecen las pautas básicas y guían el accionar de las entidades del sector público hacia la búsqueda de la efectividad, eficiencia y economía en las operaciones.

<sup>(1)</sup> Ingeniero de Sistemas.

Doctorando en Sistemas, UNFV

<sup>(2)</sup> Jefe de la Oficina de Informática.

Facultad de Ingeniería Industrial, UNSM

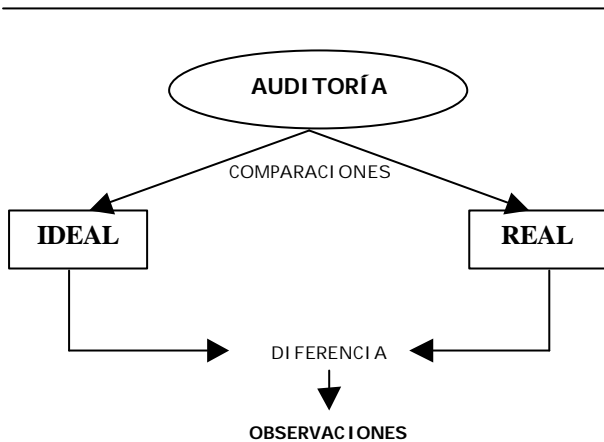


Figura 1. Esquema del concepto clásico de Auditoría

Las normas de control interno para sistemas computarizados pertenecen a la categoría 500 de las Normas de Control Interno para el Sector Público y se indican a continuación:

- 500-01 Organización del área informática
- 500-02 Plan de sistemas de información
- 500-03 Controles de datos fuente, de operación y de salida
- 500-04 Mantenimiento de equipos de cómputo
- 500-05 Seguridad de programas, de datos y equipos de cómputo
- 500-06 Plan de contingencias
- 500-07 Aplicación de técnicas de Intranet
- 500-08 Gestión óptima de software adquirido a medida por entidades públicas

### CONCEPCIÓN DE LA PROPUESTA DE AUDITORÍA INFORMÁTICA

Según Alonso Hernández García, "conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas."

De aquí se deduce la importancia de establecer una opinión objetiva, fundada en las evidencias encontradas, sobre las diferencias existentes entre el planteamiento del funcionamiento de cualquier área a auditar y su ejecución real en la organización, y comunicarlas a las personas correspondientes.

Se plantea que una de las formas de Auditoría Informática aplicado a Entidades Públicas es el proceso orientado a la identificación

de riesgos y controles en la gestión de las tecnologías de información, para su efectivo apoyo al logro de los objetivos de la institución, para el cumplimiento de sus metas estratégicas, asociado a la nueva economía digital en la que se desenvuelven (Ver Figura 2).

Por un lado la identificación de riesgos nos sirve para determinar el nivel de exposición de la institución al inadecuado uso de los servicios que brinda la tecnología de la información; pero además permite gestionar los riesgos, implementando controles que están orientados a evitarlos, transferirlos, reducirlos o asumirlos gerencialmente.

Por tanto, es necesario definir ambos conceptos: riesgos y controles, para fines del trabajo de investigación:

- a. **Riesgo:** Un riesgo impide que la Entidad logre alcanzar los objetivos establecidos como negocio y que en el tiempo dicha situación genere debilidades en el control interno. Los riesgos se agrupan de acuerdo a su impacto en la institución.
- b. **Control:** Un control establece las medidas implementadas en las Entidad con la finalidad de reducir los riesgos existentes y proteger los activos más importantes.

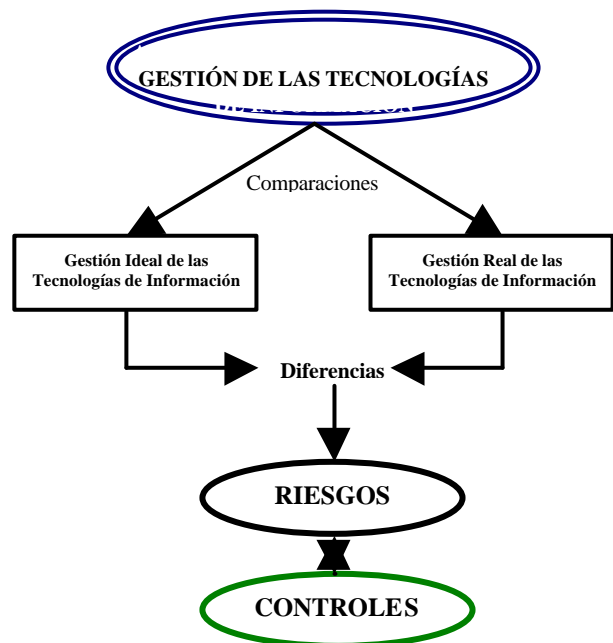


Figura 2. Esquema de Auditoría Informática de la gestión de tecnologías de información

En la Figura 3 se muestra la estrategia utilizada para la implementación de las mejores prácticas de control, es un proceso de benchmarking, que toma en cuenta las mejores recomendaciones internacionales, como las contenidas en el COBIT, las utilizadas por empresas de prestigio internacional, las normas internacionales de auditoría, entre otros; los que permiten obtener altos niveles de seguridad, fiabilidad y conformidad en la gestión de la tecnología de la información.

Los riesgos de tecnología de información que afectan a las Entidades Públicas están relacionados con 3 aspectos básicamente:

- a. **Dependencia en el uso de tecnología de información:** Relacionada con el uso que efectúa la Entidad y la importancia que representa para el desarrollo de sus operaciones
- b. **Confiablez en el uso de tecnología de información:** Relacionada con resultados del procesamiento de datos y que no requieren trabajo manual por los usuarios para completar la información.
- c. **Cambios en la tecnología de información:** Relacionado con la automatización de los procesos principales de la Entidad y la adecuación de esos procesos automatizados a nuevas necesidades de la Entidad motivados por regulación o por modernización para mantenerse competitivos o lograr su acreditación.

Para la evaluación de los controles se utilizan 4 grandes áreas:

- a. **Administración de los recursos de TI:** Para asegurar que la Entidad utilice tecnología de información bajo criterios de costo-beneficio, considerando las necesidades de automatización y adecuación de cambios del entorno en que se desenvuelve.
- b. **Seguridad Física y Seguridad de Información:** Para garantizar que el ambiente en el que los sistemas funcionan protege su confidencialidad, integridad y confiabilidad, la reducción al mínimo del riesgo de que ocurran daños accidentales o intencionales a los equipos.

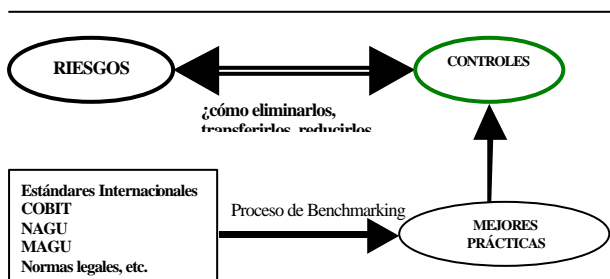


Figura 3. Esquema de implementación de controles

- c. **Desarrollo y Mantenimiento de Sistemas de Información de la Entidad:** Para garantizar la disponibilidad de los sistemas cuando se necesiten, que se controle la integridad de los datos y que satisfagan a los usuarios.
- d. **Continuidad de SI de la Entidad:** Reducir al mínimo la posibilidad de que ocurra un desastre total y garantizar que el negocio pueda reanudar sus operaciones con efectividad en caso de que ya no se disponga de las instalaciones de procesamiento existentes.

A continuación se presenta en la Figura 4, la Visión Sistémica de la Metodología propuesta, donde se puede apreciar al área de Informática de la Entidad, no como un departamento de la organización sino más bien como el entorno informático.

El proceso de auditoría, muestra claramente dos áreas bien definidas: el Área de Riesgos y el Área de Control. Los riesgos identificados nos llevarán automáticamente a definir las áreas de control; de similar modo, las áreas de control deben de ser evaluadas para determinar si los esfuerzos de la Entidad están siendo orientados a cubrir áreas de riesgo y no se presente el caso de que dichos esfuerzos estén mal orientados.

La tercera parte de este diagrama muestra la comparación entre las Áreas de Control y las Mejores Prácticas de Control; esto significa que debemos de realizar un proceso de benchmarking con la finalidad de asegurarnos que las Entidades Públicas, donde el gobierno ha realizado grandes inversiones en tecnologías de la información, estos, estén siendo utilizados y protegidos eficientemente, para ello tomaremos como referencia aquellas recomendaciones de Organismos Internacionales que orientan la gestión de Auditoría Informática en el Mundo tal como ISACAF, el COBIT, Firmas Auditoras de prestigio internacional, las NAGU, las MAGU, entre otras.

Finalmente, la visión sistémica muestra los factores del entorno que afectan de alguna manera la gestión de la tecnología de la información en las Entidades Públicas.

## CONCLUSIONES

La metodología propuesta permite revisar el uso de la tecnología de información en la Entidad, utilizando técnicas modernas para la recopilación de información y análisis detallado, con la finalidad de identificar los riesgos y evaluar los controles en el uso de las mismas.

La Auditoría Informática permite a la Entidad Pública buscar los medios para alcanzar los estándares internacionales en el uso

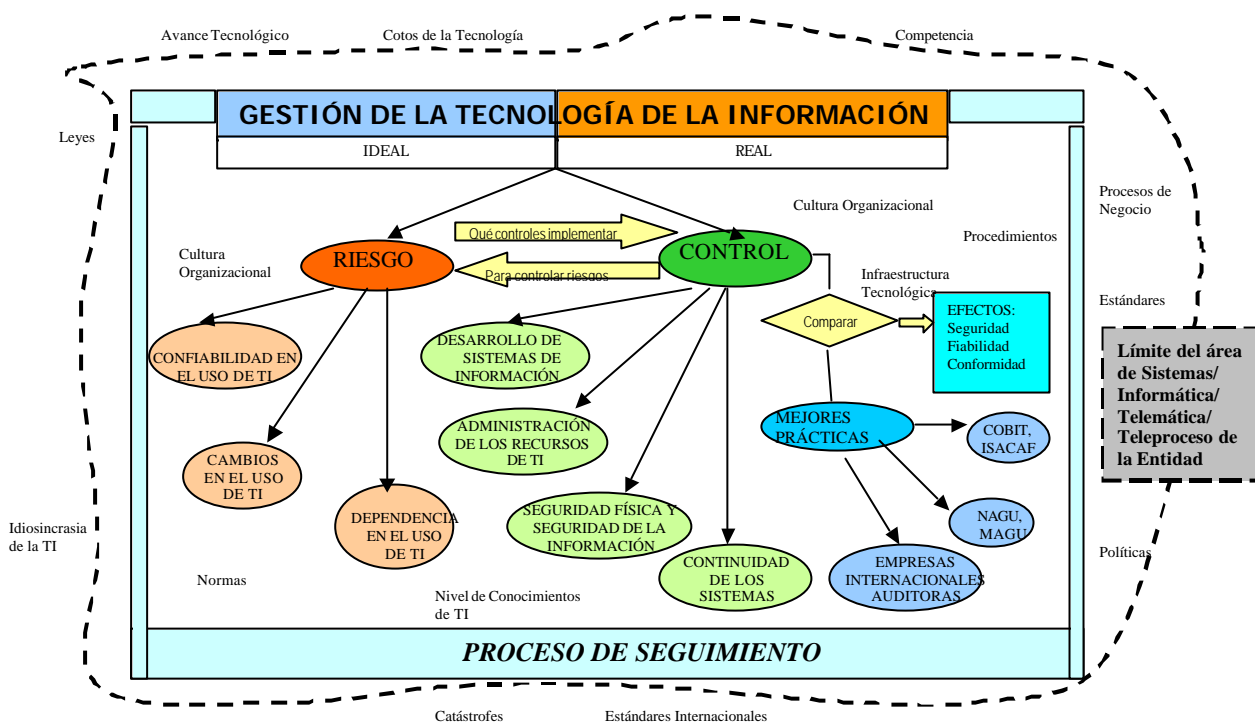


Figura 4. Visión sistemática de la auditoría informática

adecuado de las tecnologías de información, con miras a una certificación de calidad. Pone al descubierto si los esfuerzos de la Entidad están correctamente orientados a controlar los riesgos de mayor impacto y a redireccionar aquellos esfuerzos orientados a áreas que no representan riesgos.

La estrategia utilizada para la implementación de las mejores prácticas de control, es un proceso de benchmarking, que toma en cuenta las mejores recomendaciones internacionales de instituciones que orientan las auditorías informáticas a nivel mundial, las normas contenidas en el COBIT, las utilizadas por empresas de prestigio internacional, las normas internacionales de auditoría, entre otros; los que permiten obtener altos niveles de seguridad, fiabilidad y conformidad en la gestión de la tecnología de la información.

## BIBLIOGRAFÍA

1. Derrien, Y. (1994), Técnicas de Auditoría Informática. Marcombo, Barcelona.
2. Echenique García, José Antonio. (1995), Auditoría en Informática. Edit. Mc Graw Hill, México.
3. Ferreyros Morón, Juan A. (1995), Informática Contable y Auditoría de Sistemas. Edit. La Senda. Perú.
4. Gil Peuchan, Ignacio. (1999), Sistemas y Tecnologías de la Información para la Gestión. Edit. McGraw Hill. Madrid-España.
5. Hernández, Roberto; Fernández, Carlos; Baptista, Pilar. (1998), Metodología de la investigación. Edit. Mc Graw Hill, México.
6. IBM del Perú. (1998), Control y Auditoría de Sistemas de Información. Departamento de Educación de IBM del Perú S.A.
7. IBM del Perú. (1998), Seguridad en Sistemas de Información. Departamento de Educación de IBM del Perú S.A.
8. INEI. (1996), Auditoría Informática. Publicación del Instituto Nacional de Estadística e Informática del Perú.
9. Murphy, David. (1998), La auditoría de sistemas informáticos. Temas Avanzados. Documento hecho en la Escuela Nacional de Control. Contraloría General de la República.