UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE INGENIERIA INDUSTRIAL Y DE SISTEMAS
SECCION DE POST GRADO EN INGENIERIA DE SISTEMAS

METODOLOGIA PARA AUDITORÍA

INFORMATICA EN ENTIDADES PÚBLICAS

TESIS

PARA OPTAR EL GRADO DE MAESTRO EN CIENCIAS CON MENCIÓN EN INGENIERÍA DE SISTEMAS

ING° GUADALUPE RAMÍREZ REYES

LIMA – PERU
2002

INDICE

Pág. Nº

DESCRIPTORES TEMÁTICOS

- AUDITORÍA
- AUDITORÍA INFORMÁTICA
- AUDITORÍA DE SISTEMAS
- COBIT
- METODOLOGÍAS DE AUDITORÍA INFORMÁTICA
- RIESGO EL USO DE TECNOLOGÍAS DE INFORMACIÓN
- CONTROLES EN EL USO DE TECNOLOGÍAS DE INFORMACIÓN
- NORMATIVIDAD LEGAL INFORMÁTICA
- NORMAS TÉCNICAS DE CONTROL INTERNO INFORMÁTICO
- ORGZANIZACIÓN DE LOS SERVICIOS INFORMÁTICOS
- TÉCNICAS DE EVALUACIÓN
- AUDITORÍA DE LA GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

RESUMEN EJECUTIVO

Una de las principales preocupaciones de las Entidades Públicas que han realizado esfuerzos en la implementación de tecnologías de información, es su administración, control y mantenimiento; frente a ello se 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.

El Objetivo del presente trabajo de investigación fue diseñar una metodología para la ejecución de una auditoria informática en las entidades públicas peruanas; para su realización se ha utilizado la Metodología de la Investigación en Acción y el Método de Análisis y Síntesis; mientras que las técnicas fueron: entrevistas, observación, estudio de documentación, matrices de evaluación y la aplicación de cuestionarios.

Para establecer una propuesta de modelo de metodología se han considerado dos aspectos básicos e importantes relacionados con la estructura de control interno: Identificación de áreas de riesgo y la identificación de áreas de control.

Se ha seleccionado a la Universidad Nacional "Hermilio Valdizán" de Huánuco como modelo para el desarrollo de nuestra metodología.

La Auditoría Informática es un medio que dispone la Entidad Pública para gestionar los riesgos y controles de la tecnología de información. Por otro lado, el diseño de los cuestionarios, permite recopilar información acerca de las causas que motivaron al auditor a calificar de riesgo a un área, el mismo que servirá para realizar el seguimiento y como punto de partida para posteriores auditorías.

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.

INTRODUCCIÓN

Cada vez un mayor número de Entidades Públicas consideran que la información y la tecnología asociada a ella representan uno de sus activos más importantes y de igual modo que para los otros activos de la Entidad, exigen los mismos requerimientos de calidad, control, seguridad e información; por lo que se hace necesario un control permanente.

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 nace como apoyo a la labor del auditor financiero, pero debido al desarrollo explosivo de la tecnología de información en los últimos decenios, se convierte en el objeto a auditar. De esta manera, la auditoría informática ha evolucionado conjuntamente con las tecnologías de la información y su ritmo de crecimiento va de la mano con el avance tecnológico.

La Auditoría Informática se constituye en una herramienta que gestiona la tecnología de la información en las entidades, a través de auditorìas internas y externas.

El presente trabajo de investigación 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.

En el primer capítulo se presenta la problemática actual, los antecedentes y la importancia del planteamiento del problema. A continuación se plantean los objetivos del trabajo de investigación y las metodologías que se utilizarán para su desarrollo.

El segundo capítulo está orientado a mostrar el marco teórico que da el sustento y rigor científico al trabajo, presenta y cuestiona las teorías existentes en el campo de la auditoría informática.

El tercer capítulo presenta el diseño metodológico, indicando las dos grandes áreas de evaluación: riesgos y controles. Hace una detallada explicación de los aspectos importantes a evaluar, de los métodos y técnicas que se utilizarán durante el proceso de auditoría y presenta las etapas de ejecución de la misma, indicando las ventajas de cada etapa, los objetivos que se persiguen y las estrategias a utilizar. Además incluye una visión sistémica del diseño metodológico de auditoría informática.

El cuarto capítulo desarrolla la primera etapa de la Auditoría Informática, referida al entendimiento de la empresa a auditar, que para el presente trabajo de investigación se realizó en la Universidad Nacional de Huánuco Hermilio Valdizán.

El quinto capítulo desarrolla la etapa de aplicación de los cuestionarios con fines de identificación de los riesgos y evaluación de controles en el uso de la tecnología de información, teniendo como referencia los resultados obtenidos en la primera etapa.

A continuación se presenta el Informe Final, que incluye las principales observaciones y la medición del impacto de los riesgos más importantes.

Finalmente se presentan las conclusiones y recomendaciones del presente trabajo de investigación y su aplicación en la Universidad Nacional Hermilio Valdizán de Huánuco.

CAPÍTULO I

GENERALIDADES

1.1. PLANTEAMIENTO DEL PROBLEMA

Las empresas y organizaciones enfrentan cambios de orden económico, industrial, social y tecnológico por lo que deben adaptarse rápidamente a las nuevas circunstancias para sobrevivir. Cada vez un mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes y de igual modo que para los otros activos de la empresa, exigen los mismos requerimientos de calidad, control, seguridad e información.

Sin embargo, en términos generales, podemos decir que a pesar de los grandes adelantos tecnológicos, la situación actual de los sistemas de información en las instituciones se caracterizan frecuentemente por una falta de asimilación de las nuevas tecnologías, por una infrautilización de los equipos informáticos, descontento generalizado de los usuarios, por una obsolescencia de las aplicaciones informáticas actuales, por una falta de planificación de los sistemas de información, y por soluciones planteadas parcialmente y no integralmente, creando islotes de mecanización y de procesos manuales difíciles de controlar y caros de mantener. En definitiva por una falta de estándares y metodologías, por una falta de formación y cultura generalizada, sobre todo en los aspectos de control, seguridad y auditoría informática.

La auditoria informática ha aportado soluciones en el pasado a estos problemas, pero se ha realizado sólo en grandes empresas y en la mayoría de los casos como un complemento a la auditoria financiera. Sin embargo debido al mayor impacto que van adquiriendo las tecnologías de la información en las empresas, la

auditoría es necesaria y su aplicación se hace imprescindible en cualquier empresa que haya realizado inversiones en el manejo de su información.

Los aspectos normativos y estándares informáticos deben encontrarse acorde a lo establecido por las entidades responsables como la Contraloría General de la República, el Instituto Nacional de Estadística e Informática, el Ministerio de Economía y Finanzas y las establecidas por cada entidad; sin embargo muchas veces estas normas no llegan a aplicarse eficientemente poniendo en grave riesgo la inversión en este tipo de activos como son los sistemas de información y las tecnologías que las soportan.

Una de las principales preocupaciones de las empresas al efectuar inversiones importantes en materia de tecnología de la información, es que la inversión no da soluciones inmediatas tangibles y medibles, y allí donde se veía una oportunidad de mejora, realmente estamos creando un problema difícil de administrar y controlar. Es posible, entonces, ¿evaluar los riesgos y controles relacionados con el uso de tecnologías de la información en las empresas públicas? y si es posible identificar los riesgos, es necesario realizar planteamientos para mitigar los riesgos existentes y evitar un impacto económico adverso.

No preguntamos ¿el diseño de una metodología y la determinación de técnicas que permitan la implementación de la metodología permitirá realizar una auditoría informática eficiente en las entidades públicas?, ¿la identificación de riesgos potenciales en el uso de sistemas y tecnologías de la información, permitirá tomar decisiones para el mejor uso de las mismas?, ¿la determinación de los objetivos de control que respondan a las normas ayudará a un mejor control de los sistemas y tecnologías de la información? Y finalmente ¿el diseño de planes de contingencia son útiles para mantener operativo los sistemas de información en la empresa ante cualquier eventualidad?.

1. 2. OBJETIVOS DE LA INVESTIGACIÓN

OBJETIVO GENERAL

Diseñar una metodología para la auditoria informática en las entidades públicas peruanas.

OBJETIVOS ESPECÍFICOS

- Identificar riesgos en el uso de tecnologías de la información .
- Evaluar los controles en el uso de tecnología de información.
- Evaluar técnicas que permitan implementar la metodología diseñada.
- Aplicar la metodología en la Universidad Nacional Hermilio Valdizán de Huánuco.

1.3. IMPORTANCIA DEL PROBLEMA

Los temas relativos a la auditoria informática cada día cobran mayor importancia, tanto a nivel nacional como internacional, debido a que la información se ha convertido en el activo más importante de las empresas, llegando a representar su principal ventaja estratégica, en la que se invierten considerables sumas de dinero y tiempo en la creación de sistemas de información y tecnologías que las soporten, con el fin de obtener la mayor productividad y calidad.

El hecho de realizar una auditoría informática es importante, debido a que dependiendo de las técnicas y herramientas que se utilizan permiten evaluar riesgos y controles relacionados con el uso de la tecnología de la información, para determinar la manera de mitigar estos riesgos y evitar el impacto adverso de los mismos.

La implementación de las mejoras planteadas buscan mantener en óptimas condiciones los sistemas y tecnologías de información a fin de que la empresa pueda responder rápidamente a las condiciones tan cambiantes del medio marcando la diferencia con respecto a la competencia, constituyéndose en una empresa pública flexible a los cambios del entorno y acreditada en su sector.

Por otro lado es importante resaltar que la normatividad es general y debido a que los avances tecnológicos actualmente son acelerados y mientras se intenta diseñar un sistema de control de los mismos en una empresa, estos ya fueron renovados, de allí la importancia de una metodología flexible que permita capturar e incorporar estos avances y determinar objetivos de control que garanticen la eficiencia y eficacia en el uso de las tecnologías y sistemas de información.

Es necesario diseñar una metodología que se adecue a la realidad de nuestras entidades públicas peruanas y que sirva de patrón para el logro de auditorías informáticas eficientes, mediante el uso de técnicas adecuadas. Por otro lado servirá

para aquellas instituciones que intentan crear el departamento de control interno de informática o auditoría interna de informática como para las auditorías externas.

La ejecución de este trabajo de investigación permitirá establecer claramente los objetos de control, acorde con las normas emitidas por los órganos de control como son la Contraloría General de la República, el Instituto Nacional de Estadística e Informática, el Ministerio de Economía y Finanzas, etc. que efectivamente evalúen su cumplimiento y eliminen los riesgos potenciales en el uso de los sistemas y tecnologías de información.

1.4. PLANTEAMIENTO DE HIPÓTESIS

- El diseño de una metodología y la elección de técnicas adecuadas para su implementación; permitirá la ejecución de una auditoría informática que identifique riesgos y evalúe controles en el uso de tecnologías de información acorde con el contexto en el que se desenvuelven las entidades públicas peruanas.

1.5. ANTECEDENTES DEL PROBLEMA

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mediante la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría que son:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

El auditor es responsable de revisar e informar a la dirección de la organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Gloria Sánchez Valriberas[1] (Responsable del grupo de Auditoría Informática del Grupo Cajas de Madrid), establece tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficacia, utilidad, fiabilidad y seguridad de los equipos de información.

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software, y como no, la auditoría de los sistemas de información.

Una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno solo, para obtener resultados homogéneos en equipos de trabajo heterogéneos

El Instituto Nacional de Estadística e Informática[2], en su publicación sobre Auditoría Informática, menciona que existen cuatro áreas generales de la auditoría informática que son:

Auditoría Informática de usuario

Auditoría Informática de Actividades Internas

Auditoría Informática de Dirección

Auditoría de Seguridad

Dentro de estas áreas generales existen otras divisiones en las que la Auditoría Informática se subdivide, estas son: auditorías de explotación, de sistemas,

[1] SÁNCHEZ VALRIBERAS, Gloria. Control Interno y Auditoría Informática. Coautor de Piattini y Peso. Auditoría Informática. Pág. 27-29

[2] INEI. Auditoría Informática. Publicación del Instituto Nacional de Estadística e Informática del Perú. Pág. 5-15.

de comunicaciones, de desarrollo de proyectos; conformando así, las áreas específicas de la Auditoría Informática más importantes.

El INEI[3] plantea además un método de trabajo, dividido en fases:

- Determinar los alcances y objetivos.
- Análisis del ambiente a auditar y el entorno auditable.
- Determinar los recursos de la auditoría informática.
- Establecer cuáles son los recursos mínimos a emplear en la auditoría.
- Elaboración y planteamiento del plan de trabajo y de los programas.
- Actividades a realizar en la auditoría
- Elaboración del informe final.
- Elaboración de la carta de introducción correspondiente al informe final.

Sería importante señalar las técnicas y herramientas que se utilizarán en cada fase, pero esto va a depender mucho del tipo de organización en estudio, de los sistemas de información que maneje y de las tecnologías de información involucradas.

Jacinto Gómez Marín [10] en su informe de suficiencia profesional, presenta una auditoría realizada en el Instituto Peruano de Seguridad Social, donde plantea, las siguientes fases

- Planeamiento
- Ejecución de la revisión
- Ejecución de la Verificación
- Elaboración del Informe

Lo que se plantea en este trabajo de investigación es realizar una metodología aplicable a la auditoría informática de las universidades públicas peruanas, la misma que será llevada a cabo en la Universidad Nacional Hermilio Valdizán de Huánuco y que pretende verificar y evaluar el uso de los recursos informáticos tanto de sistemas como de equipos, procedimientos y funcionamiento de la Dirección de Informática de la institución, que conlleve a la seguridad y confiabilidad de la información que se

[3] Ibid. Pág. 12-17

ingresa, procesa y produce; así como su utilización más eficiente y segura de la información para que sirva realmente a la toma de decisiones en la institución.

Por otro lado se verificará la existencia y aplicación de las normas y procedimientos establecidos por órganos rectores, normativos y los definidos por la institución misma, para minimizar los riesgos por mal uso en equipos, sistemas, datos y comunicaciones, finalmente promover el mejoramiento de los sistemas de control y calidad de la información generada por los recursos informáticos.

1.6. METODOLOGÍA

En las distintas etapas del desarrollo de la tesis se irán utilizando algunas metodologías que permitan organizar el proceso de investigación, ir controlando los resultados que se vayan obteniendo y presentar posibles soluciones al problema para una oportuna y correcta toma de decisiones.

- **Metodología de la Investigación en Acción**

  Planteado por Chekland[4], menciona que la investigación en acción permite que el investigador se transforme en un participante en la acción y el proceso de cambio en sí se vuelve el objeto en estudio de la investigación. Los roles del "investigador" y "objeto de estudio" realmente no son fijos, sino que se intercambian; es decir, los objetos de estudio se vuelven investigadores y los investigadores se convierten en hombres de acción.

  La investigación en acción incluye la investigación pura, la investigación de objeto básico, investigación de evaluación y la investigación aplicada, la intención es siempre estar involucrado en un proceso de cambio en el sistema mismo como medio para la acción práctica que pretende resolver un problema.

- **Método de Análisis y Síntesis**

  Mientras que el análisis es la descomposición de un todo en sus elementos, la síntesis es una totalidad que contiene todo el sistema de relaciones. El análisis

[4] CHECKLAND, Peter. Pensamiento de Sistemas, Práctica de Sistemas. Citado por Gamboa. Tesis. Integración del Planeamiento Estratégico de Negocios con las Tecnologías y Sistemas de Información. Pág. 50-51

presupone la síntesis y viceversa; es decir, son correlativa y absolutamente inseparables. Estos métodos se utilizaran, en el tratamiento de los datos.

Las técnicas que se utilizarán para la recopilación de la información serán:

Entrevistas

Observación

Estudio de documentación

Matrices de evaluación

Aplicación de Cuestionarios

CAPÍTULO II

MARCO TEÓRICO

2.1. EVOLUCIÓN DEL CONCEPTO AUDITORÍA

Según Alonso Hernández García[5], "conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de un 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."

Inicialmente cuando el objeto de la auditoría, los documentos financieros a auditar, eran relativamente cortos y contenían más bien escasas operaciones, los procedimientos llamados de arriba abajo, que parten de los documentos financieros y auditan hacia abajo, hacia la evidencia de auditoría subyacente, que se verificaba en su integridad, tradicionalmente conocido por censura de cuentas o en base a las cuentas, era adecuado, suficiente y viable nos manifiesta Alonso.

Sin embargo, cuando llegó la llamada revolución cuantitativa que trajo consigo la creación de sociedades con importantes medios, que las operaciones se multiplicaran enormemente y que la gestión y propiedad se diferenciaran cada vez más claramente, el método tradicional resultó laborioso, tedioso, largo, ineficaz y económicamente inviable. No era posible verificar la totalidad de las muy cuantiosas operaciones y por tanto había que reducir el campo de acción del auditor a parte de la numerosa información.

[5] HERNÁNDEZ GARCÍA. Alonso. La Informática como herramienta del Auditor Financiero. Coautor de Piattini y Peso. Auditoria Informática. Pág. 4

También como nos manifiesta Dale S. Fisher[6], a partir de los primeros años del siglo XX, "la banca se convirtió en el principal usuario de las auditorías de cara al seguimiento de sus créditos y no estaba interesada en la exactitud administrativa de las cuentas sino en "la calidad y representatividad de los balances".

Este nuevo planteamiento trae implícito un riesgo evidente, al no verificarse la totalidad de los movimientos. Los controles establecidos por la entidad auditada pudieran permitir que se produjeran irregularidades, potencialmente significativas, causales o voluntarias.

Al no someterse a revisión todas y cada una de las operaciones, cabe la posibilidad de que se escape a la atención del auditor alguna de aquellas irregularidades.

El auditor tiene entonces el cometido irrenunciable de mantener el riesgo de que esto ocurra dentro de los límites tolerables.

Alonso Hernández García[7], plantea la siguiente representación aritmética:

R(c) x R(d) = S(e)

R(c): Riesgo en el proceso o riesgo de control

R(d): Riesgo de detección

S(e): Constante o parámetro admisible en que se desea mantener el riesgo de auditoría.

De ahí que nace y se justifica la imposición de Normas Técnicas que establecen que la revisión del sistema tiene por objeto el que sirva como base para las pruebas de cumplimiento y para la evaluación del sistema.

En este sentido las Normas de Auditoría en su apartado 2.4.34 (tomado del COBIT[8]), explican que el riesgo final del auditor es una combinación de dos riesgos separados:

- El primero de estos está constituido por aquellos errores de importancia que ocurran en el proceso contable, del cual se obtienen las cuentas anuales.

[6] Ibid. Pág. 6
[7] Ibid. Pág. 6-7
[8] COBIT. Normas de Auditoría Informática. Pág. 24

- El segundo riesgo es de que cualquier error de importancia que pueda existir sea o no detectado por el examen del auditor.

El auditor confía en:

- En el control interno establecido por la entidad auditada para reducir el primer riesgo
- En sus pruebas de detalle y en sus otros procedimientos para disminuir el segundo riesgo.

A partir de 1950 la información se convierte en una herramienta muy importante en las labores de auditoría financiera ya que permite llevar a cabo en forma rápida y precisa operaciones que manualmente consumirían demasiados recursos.

Sin embargo, al convertirse los sistemas de información de la empresa cada vez más dependientes de los ordenadores surge la necesidad de verificar que los sistemas informáticos funcionen correctamente, a finales de los años 60 se descubren casos de fraude cometidos con ayuda del ordenador, surge la necesidad de verificar el funcionamiento correcto, eficaz y eficiente de la información.

En el trabajo presentado por The Canadian Institute of Chartered Accountants[9], una institución de reconocido prestigio internacional, plantea la cuestión de cuáles son actualmente los "libros" o soporte de los documentos financieros objeto de la labor del auditor en un entorno informatizado, y concluye que dichos libros están materializados en los archivos electrónicos, es decir los archivos creados y mantenidos en forma electrónica por las aplicaciones contables.

El objetos es distinto, está en un soporte diferente, se ha introducido la Tecnología de la Información, este cambio trae consecuencias de gran calado en cuanto a procedimientos de auditoría financiera.

Se presenta la alternativa al auditor de utilizar los listados procedentes de los referidos archivos magnéticos como fuente de información o acceder directamente a los archivos electrónicos y proceder a su análisis en forma electrónica.

[9] HERNÁNDEZ GARCÍA. ALONSO. Log. Cit. Pág. 8

Aparecen entonces los CAATS (Técnicas de Auditoría Asistidas por Ordenador), es la misma tecnología de la información que da solución y proporciona los medios para ejecutar la auditoría en forma eficiente y directa. Charles. H. Le Grand[10] en su trabajo de investigación sobre el uso de los CAATTS en auditoría manifiesta que estas herramientas deben ser usadas como medios para realizar la auditoría y presenta una clasificación para su uso como sigue:

- Análisis de riesgos
- Inventario del universo de auditoría
- Planeamiento y programación
- Gerencia de proyectos y seguimiento de la auditoría
- Base de Datos personal y habilidades de auditoría
- Librería para auditoría de referencia
- Comunicaciones
- Seguimiento de resultados / Hallazgos
- Internet

Entonces, puedo afirmar claramente que la introducción de las tecnologías de información en los sistemas de información afecta a los auditores en forma dual porque:

1ero. Cambia el soporte del objeto de su actividad

2do. Posibilita la utilización de medios informatizados para la realización de sus procedimientos.

Si desmenuzamos el contenido de la auditoría y su evolución podemos observar que el concepto permanece inamovible y son su objeto y finalidad lo que puede variar.

[10] LE GRAND. Charles; LEY PARKER, Xenia; HORTON, Tomas. Information Security Governance. clegrand@theiia.org. Pág 3.

De todo ello se desprende la nueva situación del auditor financiero: la de aplicar procedimientos que utilizan técnicas asistidas por ordenador a un objeto consistente en un sistema de información basada en las Tecnologías de la Información.

Habiéndose implantando el uso de las tecnologías de la información en el manejo contable de los sistemas de información como respuesta al gran volumen de información que se manejaba, es necesario determinar si se está usando correctamente la TI (Tecnología de la Información), si los resultados que arroja son confiables, oportunos, de calidad, perdurables en el tiempo; por tanto nace la necesidad de auditar a las tecnologías de la información y con ello nace el nuevo concepto de auditoría informática, del cual nos ocuparemos en seguida.

A continuación presento el siguiente esquema de su evolución.

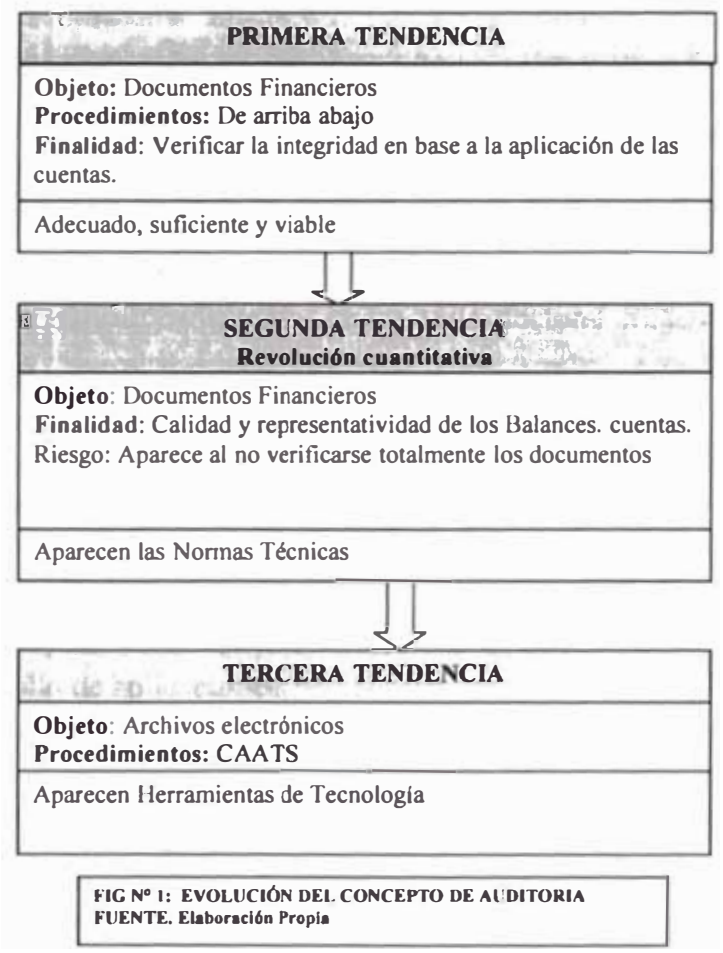


FIG Nº 1: EVOLUCIÓN DEL CONCEPTO DE AUDITORIA
FUENTE. Elaboración Propia

2.2. CONCEPTO DE AUDITORÍA INFORMÁTICA

Dentro del abanico de definiciones, podemos citar a las siguientes:

A) La de A.J.Thomas[11] en el sentido de que "la auditoría informática, que es una parte integrante de la auditoría, se estudia por separado para tratar problemas específicos y para aprovechar los recursos del personal. La auditoría informática debe realizarse dentro del marco de la auditoría general. El cometido de la auditoría informática se puede dividir en:

> Un estudio del sistema y un análisis de los controles organizativos y operativos del departamento de informática.
>
> Una investigación y análisis de los sistemas de aplicación que se estén desarrollando o que ya estén implantados.
>
> La realización de auditorías de datos reales y de resultados de los sistemas que se estén utilizando.
>
> La realización de auditoría de eficiencia y eficacia."

B) Incluyendo la de un destacado miembro de la O.A.I. (Organización de Auditoría Informática), Miguel Angel Ramos[12], que define, según sus manifestaciones simplificadamente, en su tesis doctoral Sistemas Expertos aplicados a la Auditoría Informática la define como "la revisión de la propia informática y de su entorno" y desglosa sin carácter exhaustivo que las actividades a que da lugar esta definición pueden ser:

> Análisis de riesgos.
> Planes de contingencia.
> Desarrollo de aplicaciones.
> Asesoramiento en paquetes de seguridad.
> Revisión de controles y cumplimiento de lo mismos, así como de las normas legales aplicables.
> Evaluación de la gestión de los recursos informáticos.

[11] HERNÁNDEZ GARCÍA. ALONSO. Log. Cit. Pág. 10
[12] RAMOS GONZÁLES, Miguel Angel. Auditoría de la Seguridad. Coautor de Piattini y Peso. Auditoría Informática. Pág. 11.

C) La de J.J.Acha[13] que la define como "Un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente".

De ellas se desprende que tienden a abarcar conceptos tanto de auditoría como de consultoría. Mientras que algunos autores como José María Gonzáles Zubieta[14] (Miembro de la ISACA, del OAI y del ANSEC) hace énfasis en que debe diferenciarse claramente la actuación del consultor del auditor interno y del auditor externo cuando manifiesta: "que la metodología del análisis de riesgo utilizada en auditorías internas llegan a ser utilizadas por el auditor externo" siendo esto una aberración según sus propias palabras.

Es de mi opinión que las tendencias hoy en día son de hacer de la auditoría también un aporte de consultoría.

De esta manera el papel de la auditoría informática se convierte en algo más que una clásica definición del auditor informático: "... el auditor informático es responsable para establecer los objetivos de control que reduzcan o eliminen la exposición al riesgo de control interno. Después que los objetivos de auditoría se hayan establecido, el auditor debe revisar los controles y evaluar los resultados de su revisión para determinar las áreas que requieren correcciones o mejoras".

Creo que el papel del auditor informático tiene que dejar de ser el de un profesional cuya única meta empresarial sea analizar el grado de implantación y cumplimiento del control interno. Las organizaciones están invirtiendo mucho dinero en sistemas de información, cada vez son más dependientes de ellos y no pueden permitirse el lujo de tener profesionales mediatizados por esquemas tradicionales, pero que hoy en día no los son a tenor de las necesidades empresariales. El concepto de control interno es importante, pero además de verificar dicho control, el auditor

[13] Hernández García. Alonso. Log. Cit. Pág. 12
[14] Gonzales Zubieta, Metodología de Control Interno, Seguridad y Auditoría Informática. Coautor de Piattini y Peso. Auditoría Informática. Pág.49.

tiene la obligación de convertirse un poco en consultor y en ayuda del auditado, dándole ideas de cómo establecer procedimientos de seguridad, control interno, efectividad, eficacia y medición del riesgo empresarial.

D) Finalmente Ron Weber, en su libro EDP Auditing, Conceptual Foundations and Practice", define a la que denomina "Electronic Data Process Aduting" (Auditoría de Procesos Electrónico de Datos), como el "proceso de recolección y evaluación de evidencias utilizadas para determinar cuándo un sistema informático salvaguarda sus activos, mantiene la integridad de sus datos, ejecuta eficazmente los objetivos marcados por la organización con efectividad y consume los recursos eficientemente".

Analizando estas definiciones, se puede encontrar los aspectos comunes entre ellos:

1. Examen metódico: dado que es del todo imprescindible para proceder a evaluar y verificar con éxito el servicio, objeto de estudio, seguir un plan sistematizado (obtención de información, investigación y análisis previsto según objetivos marcados) que permita llegar a conclusiones perfectamente fundamentadas.
2. Puntual y discontinuo: puntual, ya que se procede a dar un corte en el calendario para llevarla a cabo, y discontinua, en aras de buscar la objetividad (independencia) de quien la ejecuta, respecto de la empresa.
3. Verificación y evaluación de los entornos informáticos y no únicamente revisión: implícito en las definiciones se encuentra el hecho de aportar valor añadido, es decir asesorar y proponer mejoras sobre aquellas evidencias y puntos débiles detectados.
4. Destinada a la ayuda en la mejora de la seguridad, eficacia, eficiencia y rentabilidad del entorno informático de la empresa.
5. Establecer una opinión objetiva, fundada en las evidencias encontradas, sobre las diferencias existentes entre el planteamiento del funcionamiento de cualquier área de los entornos informáticos y su ejecución real en la organización, y comunicarlas a las personas correspondientes.

2.3. CLASIFICACIÓN DE LA AUDITORÍA INFORMÁTICA

Los objetivos propios de la auditoría de sistemas de información son difíciles de precisar no existiendo un acuerdo unánime al respecto, por lo que tampoco podemos delimitar con exactitud las funciones a desarrollar.

Así pues, procederé a dar una clasificación de los diferentes tipos de auditoría siguiendo los tres criterios de clasificación más frecuentes. Sustentada por Gil Peuchán[15] en su libro Sistemas y TI para la Información, Ulric J. Gelinas y Allan E.Oram en su libro Accounting Information System.

A. En función de sus objetivos.

B. Según el personal que realice la auditoría

C. Según el campo de aplicación

A) EN FUNCIÓN DE SUS OBJETIVOS

A.1. Auditoría Financiera: mediante la cual las empresas someten al examen de un experto su información económico-financiera, para asegurar su integridad y racionabilidad, en concordancia con los principios contables.
A.2. Auditoría Organizativa: encargada de evaluar los procedimientos y funciones establecidas, según las necesidades y problemas de la empresa.

A.3. Auditoría de Gestión: su misión fundamental es conocer la consistencia de los principales elementos (decisiones) de gestión en la organización.

A.4. Auditoría de Sistemas de Información: aquella actividad profesional de investigación, evaluación, dictamen y recomendación centrada en las Tecnologías de Información como actividad o fin en sí mismas, como instrumentos al servicio de otras funciones más o menos dependientes de ellas, o en ambos aspectos.

B) EN FUNCIÓN DEL PERSONAL DE AUDITORÍA

Básicamente una auditoría puede ser realizada por personas que pertenecen a la organización objeto de auditoría, como por otras ajenas a esta.

[15] GIL PEUCHAN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Pág. 58-65.

Según esta distinción podemos a las siguientes reclasificación de auditorías:

B.1. auditoría Interna: aquella en la cual el examen del sistema informático es efectuado únicamente por personas que trabajan en la organización objeto de estudio.

Sus funciones principales son:

Auditoría de apoyo a las cuentas

Auditoría operativa

Garantía de calidad

Este tipo de auditorías están generalmente poco implantadas, principalmente por la carencia de recursos asignados a ella y por su baja credibilidad exterior (nula independencia).

B.2. Auditoría Externa: aquella que es ejecutada por personal ajeno (independiente) a la organización objeto de estudio.

Tanto la Auditoría de Sistemas de Información Interna como Externa, no son sustitutivas, ya que cada una tiene su propia personalidad, ni tienen por qué ser excluyentes, sino más bien debería (en caso de coexistir) producirse una simbiosis entre ambas.

C) SEGÚN LA EXTENSIÓN DEL AMBITO DE APLICACIÓN

Según la extensión del ámbito de aplicación de la auditoría podemos proceder a una nueva clasificación de Auditoría de Sistemas de Información: Auditoría operativa y funcional, las cuales a su vez las subclasificaremos según los temas que procedan a examinar, como Auditoría de las cifras, de los procedimientos y de gestión.

C.1. Auditoría de SI Operativa:

a. Auditoría de Gestión: entendida esta como aquella orientada a controlar los elementos que definen una gestión de proyectos adecuada, establecerá los mecanismos necesarios para controlar la relación coste-eficiencia de la aplicación que se está analizando.

b. Auditoría de los Procedimientos: como aquella cuyo objetivo prioritario consiste en garantizar el exacto cumplimiento de las normas y procedimientos.

b.1. Que existan normas y procedimientos, y que en su día fueron instaurados convenientemente.

b.2. Que las pautas, recomendaciones,... se cumplen con rigor, tanto por los profesionales informáticos, como por los usuarios no informáticos de las aplicaciones en uso.

c. Auditoría de las Cifras: entendida como tal aquella que se encarga de la (i)Fiabilidad de la información utilizada y (ii)Detección de fraudes y manipulación en datos o programas.

Este tipo de auditoría, se encargará del establecimiento de aquellos controles que garanticen la fiabilidad, para lo cual deberá considerar a la organización de manera global, ya que no se puede analizar adecuadamente la información y olvidar aquellos departamentos que no están dentro del entorno informático(ventas, ...), pero que si suministran una parte importante de la información.

C.2. Auditoría del SI Funcional:

Aquella cuyo cometido principal es analizar todos los aspectos que contribuyan a que la función informática sea una herramienta eficiente al servicio de la organización, que justifica sus costes-intentando minimizarlos- y que su implantación siga criterios de racionalidad y armonía con los objetivos de la organización.

a. Auditoría de Gestión: encargada de examinar el grado de integración de la TI en la empresa.

b. Auditoría de los Procedimientos: centrada principalmente en:

- Seguridad de los locales donde esté ubicado el Centro de Procesos de Datos.
- Niveles de seguridad de hardware y software.

- Procedimientos de explotación.
- Correcta implantación y cumplimiento de las normas de trabajo.
- Fiabilidad de las aplicaciones en curso.
- Cumplimiento de plazos previstos para aplicaciones.

c. Auditoría de las Cifras: su misión es equivalente a la realizada en la auditoría operativa, es decir, establecer una serie de controles que garanticen la fiabilidad de los datos.

A continuación presento el esquema de clasificación:

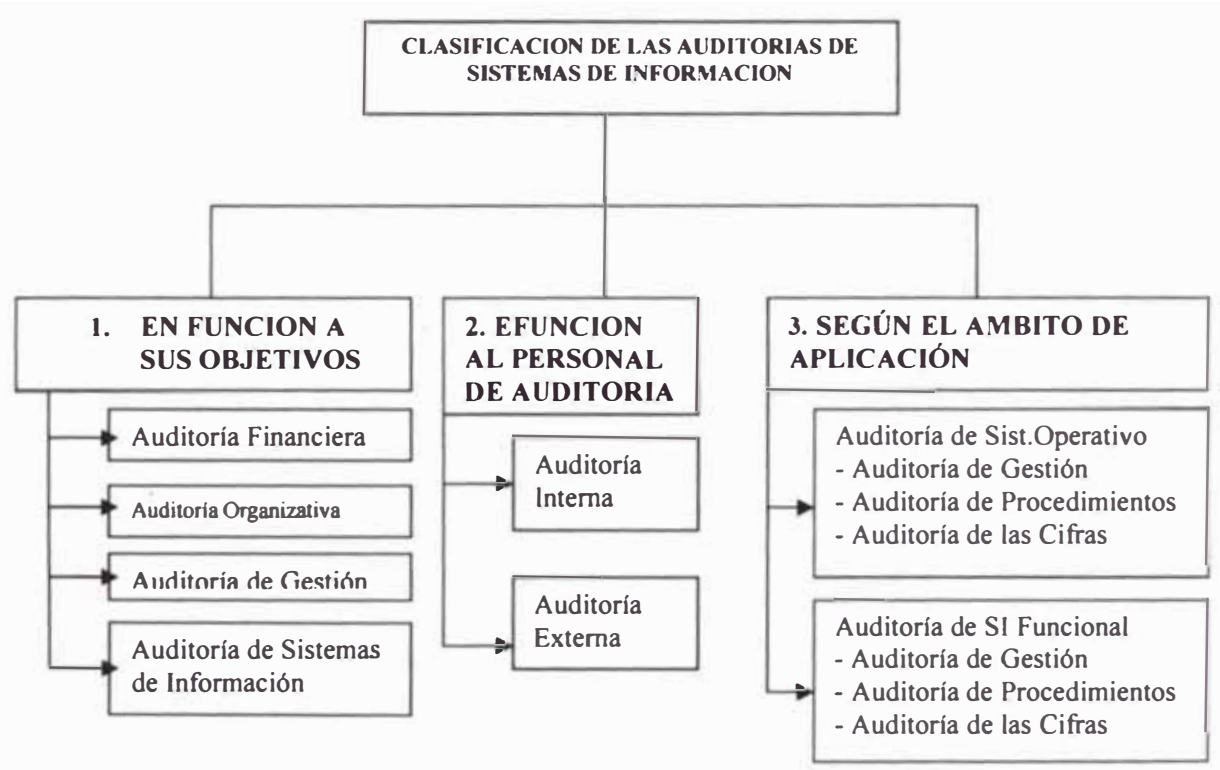


FIG. N° 2: CLASIFICACIÓN DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN.

FUENTE: Gil Peuchán. Sistemas y Tecnologías de Información

2.4. INSTITUCIONES INTERNACIONALES QUE ORIENTAN LA AUDITORÍA INFORMÁTICA A NIVEL MUNDIAL

La organización de mayor reconocimiento, encargada de la normalización de tareas y técnicas a aplicar en la función de la Auditoría de SI es la (ISACA) "Information System Audit. and Control Association" (antiguamente denominada EDPAA- Electronic Data Processing Auditors Association), fundada en 1969 en EE.UU.

En 1976 nació la EDPAF (Electronic Data Processing Auditors Foundation), dependientemente de la EDPAA, y cuyo objetivo es la difusión de información referente a los distintos aspectos de la Auditoría de Sistemas de Información.

La OAI (Organización de Auditoría Informática), constituye el capítulo español de "The ISACA", la cual como ente creado en 1987, conjuntamente por ALI (Asociación de Licenciados en Informática) y el Consejo Generadle Economistas de España, conforma la representación de la Asociación Americana en España.

Otras asociaciones internacionales que no podemos dejar de citar son:

AICPA:American Institute of Chartered Public Accountans.

IIA: Institute of Internal Auditors.

- QAI: Quality Assurance Institute.

ASQC: American Society of Quality Control.

Y en España:

ATI: Asociación de Técnicos en Informática.

REA: Registro de Economistas Auditores.

ROAC: Registro Oficial de Auditores de Cuentas.

En muchos países latinoamericanos la ISACA, la OAI, tienen sedes descentralizadas como en Chile, Colombia., México, Costa Rica, etc. En el Perú no existe sede.

Los autores más representativos en el área de auditoría informática sin duda, son los miembros de la ISACA y de la OIA. Estos miembros para ejercer las funciones de

auditoría tienen que dar exámenes para ser presentados por la OAI y ejercer las funciones de auditor en cualquier lugar del mundo con el prestigio y respaldo de la OAI.

2.5. DESARROLLO DE METODOLOGIAS DE AUDITORÍA INFORMÁTICA

Según el Diccionario de la Lengua de la Real Academia Española, MÉTODO es "modo de hacer o hacer con orden una cosa". Así mismo define el diccionario la palabra METODOLOGÍA como "conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal". Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad que llamaremos METODOLOGÍA.

Las metodología usadas por un profesional dice mucho de su forma de entender su trabajo, y están directamente relacionadas con su experiencia profesional acumulada como parte del comportamiento humano de "acierto/error".

Asimismo una metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como silo hiciera uno sólo, por lo que resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales, desarrollas a por lo más expertos, para conseguir resultados homogéneos, en equipos de trabajo heterogéneos.

Nos dice José María Gonzáles Zubieta[16], que, "la proliferación de metodologías en el mundo de la auditoría y el control informáticos se pueden observar en los primeros años de la década de los ochenta, paralelamente el nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos). Pero el uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de metodologías constituye una práctica habitual. Una de ellas es la seguridad de los sistemas de información."

---

[16] GONZÁLES ZUBIETA. José María. Metodologías de Control Interno, Seguridad y Auditoría Informática. Coautor de Piattini y Peso. Auditoría Informática. Pág. 46

Aunque de forma simplista se trata de identificar la seguridad informática a la seguridad lógica de los sistemas, nada está más lejos de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos para la informática.

El nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas destinadas a proteger y preservar la información de la entidad y sus medios de proceso.

José María Gonzáles[17] plantea la Pirámide de Valor para representar el conjunto de contramedidas que deben utilizarse en una organización para evaluarla y el papel de las metodologías de auditoría.

FIGURA Nº 3: PIRÁMIDE DE VALOR

FUENTE: José María Gonzáles Zubieta. Auditoría informática

LA NORMATIVA debe definir de forma clara y precisa todo lo que debe existir y ser cumplido, tanto desde el punto de vista conceptual,

[17] Ibid. Pág. 47-49.

como práctico, desde lo general a lo particular. Debe inspirarse estándares, políticas, marco jurídico, políticas y normas de empresa, experiencia y práctica profesional. Desarrollando la normativa, debe alcanzarse el resto del "gráfico valor". Se puede dar el caso de una normativa y su carácter disciplinario sea el único control de un riesgo, pero no es frecuente.

LA ORGANIZACIÓN la integran con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Éste es el aspecto más importante, dado que sin él, nada es posible. Se pueden establecer controles sin alguno de los demás aspectos, pero nunca sin personas, ye que son éstas las que realizan los procedimientos y desarrollan los Planes (Plan de Seguridad, Plan de contingencia, auditorías, etc.)

LAS METODOLOGÍAS, son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

LOS OBJETIVOS DE CONTROL, son los objetivos a cumplir en el control de procesos. Este concepto es el más importante después de "LA ORGANIZACIÓN", y solamente de un planeamiento correcto de los mismos saldrán unos procedimientos eficaces y realistas.

LOD PROCEDIMIENTOS DE CONTROL, son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control, y por tanto deben de estar documentados y aprobados por la Dirección. La tendencia habitual de los informáticos es la de dar más peso a la herramienta que al "control o contramedida", pero no debemos olvidar que "UNA HERRAMIENTA NUNCA ES UNA SOLUCIÓN SINO UNA AYUDA PAR CONSEGUIR UN CONTROL MEJOR". Sin la existencia de estos procedimientos, las herramientas de control son solamente un anécdota.

Dentro de la TECNOLOGÍA DE SEGURIDAD están todos los elementos, ya sean hardware o software, que ayudan a controlar un riesgo informático. Dentro de este concepto están los cifrados, autentificadotes, equipos "tolerantes de fallo", las herramientas de control, etc.

LAS HERRAMIENTAS DE CONTROL, son elementos de software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Las dos metodologías de evaluación de sistemas más generales que se han podido determinar de la exploración bibliográfica son las de ANALISIS DE RIESGO y las de AUDITORÍA INFORMÁTICA, con dos enfoques distintos. La auditoría informática sólo identifica el nivel de "exposición" por la falta de controles, mientras el análisis de riesgos facilita la "evaluación" de los riesgos y recomienda en base al costo-beneficio de las mismas.

Con esta última clasificación no estoy de acuerdo porque la tendencia debe ser de apoyar a la organización a mejorar ya sea a través de una auditoría interna o externa.

Will Ozzier[18] en su último trabajo de investigación publicado Unformation Risk Análisis, assessment and management, concluye que para cualquier método y herramienta utilizada por el auditor, deben compartirse su proceso de valoración con el análisis de riesgo para enviar mejores resultados a la dirección, porque permite una comunicación eficaz con los objetivos, indica prioridad y alcance de las auditorías. La dirección también debe ser consciente de los beneficios a ser obtenidos usando análisis de riesgo y su valoración en el contexto de los riesgos asociados con las alternativas de la planificación estratégicas para el desarrollo de la aplicación, software, hardware, comunicaciones, situación, y control de gestión. El uso de análisis de riesgo y su valoración es estratégico, mientras no necesariamente una

[18] OZIER, Will. Information Risk Análisis, Assessment and Mangemenet. Febrero 2000. woozier@pacbell.net; http://www.itaudit.org/index_search.htm. Pág. 1-5

función de la auditoría, puede ser muy rentable pero puede prevenir los riesgos potencialmente costosos.

Gonzáles Zubieta[19], presenta la siguiente clasificación de las metodologías:

Cuantitativas: Basadas en un modelo matemático numérico que ayuda a la realización del trabajo.

Cualitativas: Basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

Metodologías cuantitativas

Diseñadas para producir una lista de riesgos que pueden compararse entre si con facilidad por tener asignado unos valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos o de planes de contingencias son datos de probabilidad de ocurrencia (riesgo) de un evento que se debe extraer de un registro de incidencias donde el número de incidencias tienda al infinito o sea suficientemente grande. Esto pasa en la práctica, y se aproxima ese valor de forma subjetiva restando así rigor científico al cálculo. Pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas podríamos aceptarlo.

Por lo tanto vemos con claridad dos grandes inconvenientes que presentan estas metodologías: por una parte la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial, y por otro la imposibilidad o dificultad de evaluar económicamente todos los impactos que pueden acaecer frente a la ventaja de poder usar un modelo matemático para el análisis.

[19] Gonzáles Zubieta. José María. Log Cit. Pág. 51-52

	CUANTITATIVA	CUALITATIVA/SUBJETIVA
PROS	Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnerabilidades muy distintas. Proporciona una cifra "justificante" para cada contramedida.	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Incluye factores intangibles.
CONTRAS	Estimación de probabilidad depende de estadísticas fiables inexistentes. Estimación de las pérdidas potenciales. Metodologías estándares Difíciles de mantener o modificar. Dependencia de un profesional.	Depende fuertemente de la habilidad y calidad del personal involucrado. Puede excluir riesgos significantes desconocidos (depende de la capacidad del profesional para usar el check-list/guía). Identificación de eventos reales más claros al no tener que aplicarse probabilidades complejas de calcular. Dependencia de un profesional.

FIGURA Nº 4: COMPARACIÓN ENTRE METODOLOGÍAS CUANTITATIVAS Y CUALITATIVAS
FUENTE: Mario Piattini. Auditoría Informática

A continuación nombraré las metodologías más comunes encontradas en los trabajos de investigación y de campo.

Las metodologías más comunes de evaluación de sistemas que podemos encontrar son análisis de riesgos o de diagnósticos de seguridad, las de plan de contingencias, y las auditorías de controles generales.

El esquema básico de una metodología de análisis de riesgos es en esencia el representado en la figura, fue elaborado por Gonzáles Zubieta[20]

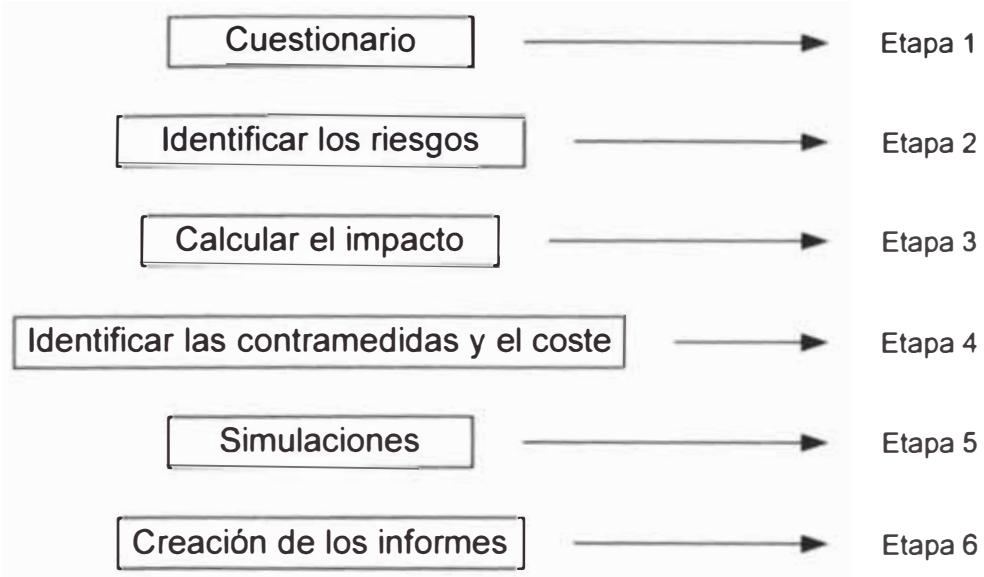


FIGURA Nº 5: ESQUEMA BÁSICO DE UNA METODOLOGÍA DE ANÁLISIS DE RIESGOS
FUENTE: José María Gonzáles Zubieta. Auditoría Informática

2.6. TENDENCIA ACTUALES DE INVESTIGACION EN AUDITORÍA INFORMÁTICA

Las áreas de aplicación de Auditoría de Sistemas de Información pueden llegar a ser muy amplias y diversas, como por ejemplo la Auditoría del desarrollo de sistemas, de la Organización y Gestión del Centro de Proceso de Datos, de las Aplicaciones, de la Seguridad (Física y Lógica), etc.

La siguiente clasificación realizada por Gil Peuchan, resulta ser muy restringida para la actual explosión que tiene el desarrollo de las tecnologías de información y por consiguiente las investigaciones están en pleno desarrollo de acuerdo con su expansión. Aquí presentamos esta clasificación.

1. AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA: la importancia de la información en las organizaciones y el elevado valor de sus activos

[20] Ibid. Pág. 53

informáticos, exige cada vez más la identificación de posibles amenazas sobre estos.

1.1. Auditoría de entornos físicos: analizando la adecuación de las instalaciones, salvaguarda ante un posible fuego o inundación, accesos, planes de contingencia, pólizas de seguro, etc.

1.2. Auditoría de la seguridad lógica: garantizando la salvaguarda en el menos dos dimensiones,

a) Acreditación de usuarios (accesos personales al sistema,...)

b) El Secreto de archivos y transacciones.

2. AUDITORÍA DE LA PLANIFICACIÓN: la auditoría de Sistemas de Información en el área de Planificación, deberá efectuarse considerándolo los tres niveles básicos en que se estructuran las organizaciones:

2.1. Nivel estratégico: (a 4 o 5 años): fijación de planes de futuro y su integración con la estrategia empresarial.

2.2. Nivel táctico: (a 1 o 2 años): fijación de un plan informático que permita ordenar prioridades según necesidades previstas.

2.3. Nivel operacional: la asociación a cada tarea de un plan operacional que realice un adecuado seguimiento de la misma.

3. AUDITORÍA DE LA ORGANIZACIÓN Y GESTIÓN DE PROCESO DE DATOS: esta auditoría persigue un análisis detallado de las estructuras organizativas, de gestión y procedimientos que tengan una relación con una adecuada organización y gestión del Centro de Procesos de Datos.

El objetivo de la Auditoría de Sistemas de Información en esta área consiste en garantizar que el responsable del Centro de Proceso de Datos, organiza, dirige y controla los recursos del mismo, tales como la dotación de Recursos Humanos, relaciones con proveedores y usuarios, la estructura del departamento, etc.

4. AREA DE EXPLOTACIÓN: la Auditoría de SI en el área de explotación persigue examinar los procedimientos seguidos en el departamento de proceso de datos en su operatividad diaria.
5. AREA DEL ENTORNO HARDWARE /SOFTWARE: el objetivo primordial de la Auditoría de Sistemas de Información en el área del entorno hardware y software, es garantizar un eficiente funcionamiento y utilidad del ordenador, garantizando su continuidad en el tiempo.

2.7. OBJETIVOS DE CONTROL ACERCA DEL USO DE TECNOLOGÍA DE INFORMACIÓN INTERNACIONALES

COBIT (Control Objetives for Information and related Techonology)

El COBIT[21], presenta normas de auditoría internacionalmente aceptada por las organizaciones dedicadas a la auditoría en el mundo, de allí la necesidad de conocerlas y aplicarlas a la metodología que se pretende implementar, puesto que presenta los Objetivos de control relacionados con la información y la tecnología

2.7.1. ANTECEDENTES

Los objetivos de control relacionados con información y tecnología "COBIT" han sido desarrollados como un estándar generalmente aplicable y aceptado para la práctica del control de tecnología de información. Está basado en los Objetivos de Control elaborados por la institución "Information Systems Audit and Control Foundation" (ISACF) y mejorados con los estándares internacionales existentes y técnicos, profesionales, regulatorios y específicos de la industria. Los objetivos de control resultantes, aplicables y aceptados en forma generalizada, han sido desarrollados para ser aplicados a los sistemas de información de toda la empresa.

[21] COBIT. Guidelines Management http://www.isaca.org. Pág. 1-53.

El término "generalmente aplicable y aceptado" es explícitamente utilizado en el mismo sentido que los Principios Contables Generalmente Aceptados (GAAP). Para los propósitos de este trabajo, "buena práctica" significa el consenso de los expertos en aspectos de eficiencia y efectividad.

El estándar es relativamente pequeño en tamaño e intenta, siempre que sea posible, ser pragmático y responder a las necesidades del negocio, siendo a la vez independiente de la plataforma técnica de tecnología de información adoptada en la organización. La necesidad de indicadores de rendimiento (normas, reglas, etc.) ha sido identificada como prioridad para las futuras mejoras que se realicen en la estructura.

2.7.2. CONTENIDO

Las organizaciones deben satisfacer con su información, como por todos sus activos, los requerimientos de calidad, información financiera y seguridad. La Gerencia debe balancear el uso de recursos disponibles incluyendo gente, instalaciones, tecnología, sistemas aplicativos y datos. Para sustentar esta responsabilidad, así como para lograr sus expectativas, la dirección debe establecer un sistema adecuado de control interno. Tal sistema o estructura debe soportar los procesos del negocio y debe ser claro sobre cómo cada actividad individual de control impacta en los recursos y satisface los requerimientos. El control, que incluye políticas, estructuras organizacionales, prácticas y procedimientos es responsabilidad de la Gerencia. Un objetivo de control es una declaración del resultado deseado o propósito a lograr al implementar procedimientos específicos de control dentro de una actividad de tecnología de información

La orientación hacia los negocios es el tema principal de COBIT. La estructura es en respuesta a la necesidad de un sistema de control interno en tecnología de información. Está diseñado no sólo para ser empleado por los usuarios y los auditores, sino también, y más importante, como una amplia "lista de revisión" para los propietarios del proceso del negocio. Cada vez más, la práctica de los negocios involucra una completa facultad en los propietarios de los procesos del negocio, de

forma tal, que tienen responsabilidad total sobre todos los aspectos del proceso del negocio. En particular, esto incluye la provisión de controles adecuados. La estructura COBIT provee una herramienta para el propietario del proceso del negocio que facilita el descargo de su responsabilidad. La estructura comienza con una premisa simple y pragmática: "Los recursos de tecnología de información necesitan ser administrados por un conjunto de procesos de tecnología agrupados naturalmente para proveer la información que necesita la empresa para el logro de sus objetivos".

Continúa con un conjunto de 32 objetivos de control de alto nivel, uno para cada proceso de tecnología de información, agrupado en cuatro dominios: Planeamiento y Organización, Adquisición e Implementación, Entrega y Soporte y Monitoreo. Esta estructura cubre todos los aspectos de la información y de la tecnología que la soporta. Al encarar estos 32 objetivos de control de alto nivel y con referencia a las políticas y estándares de la empresa, el propietario del proceso del negocio puede asegurar que se provee un sistema de control adecuado para el ambiente tecnológico. En la estructura del COBIT se destaca el impacto sobre los recursos tecnológicos junto con los requerimientos del negocio que necesitan ser satisfechos, en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. Adicionalmente, la estructura brinda definiciones para los requerimientos del negocio que son obtenidos de niveles más altos de objetivos para calidad, seguridad e información financiera según se relacionan con tecnología de información.

2.7.3. EL MODELO DE CONTROL

Hay dos clases diferentes de modelos de control disponibles actualmente, los de la clase "modelo de control del negocio " (COSO) y los más "focalizados modelos de control para Tecnología de Información" (DTI). COBIT intenta unir la brecha existente entre ambos. COBIT está entonces posicionado como más amplio para la Gerencia y para operar a un nivel más alto que los estándares tecnológicos para administración de sistemas de información. El concepto que apuntala la estructura COBIT es que el control en tecnología de información es enfocado mirando hacia la

información que se necesita en los procesos del negocio y hacia la información resultante de la aplicación combinada de recursos relacionados con tecnología, que requieren ser administrados mediante procesos de tecnología de información.

2.7.4. RECURSOS DE TECNOLOGÍA DE INFORMACIÓN

Los recursos de Tecnología de Información pueden ser definidos como sigue:

- **Datos:** Objetos en su más amplio sentido, (externos e internos), estructurados y no estructurados, gráficos, sonido, etc.
- **Sistemas de Información:** Se entiende como sistemas de información la suma de procedimientos programados y manuales.
- **Tecnología:** Cubre hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, tecnologías de comunicación, etc.
- **Instalaciones:** Recursos para albergar y soportar los sistemas de información.
- **Personal:** Habilidades del personal, capacidad, concientización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear sistemas de información y servicios.

2.7.5. REQUERIMIENTOS DE CALIDAD, FINANCIEROS Y DE SEGURIDAD

Comenzando el análisis desde los requerimientos amplios de Calidad, Financieros y Seguridad, se extrajeron siete categorías distintas, seguramente superpuestas, según el siguiente detalle:

- **Efectividad:** trata con información relevante y pertinente al proceso de negocios, así como entregada de una manera oportuna, correcta, consistente y útil.

- **Eficiencia:** concierne a la provisión de información mediante el uso óptimo (más productivo y económico) de los recursos.
- **Confidencialidad:** concierne a la protección de la información sensible respecto de la disposición no autorizada.
- **Integridad:** se relaciona con la precisión y totalidad de la información así como con su validez de acuerdo con los valores y expectativas del negocio.
- **Disponibilidad:** se refiere a que la información esté disponible cuando sea requerida por el proceso del negocio, ahora y en el futuro. También concierne a la salvaguarda de los recursos necesarios y las capacidades asociadas.
- **Cumplimiento:** trata con el cumplimiento de aquellas leyes, regulaciones y arreglos contractuales a los cuales está sujeto el proceso del negocio, ej: criterios del negocio impuestos desde el exterior.
- **Confiabilidad de la Información:** se relaciona con la provisión de información apropiada a la Gerencia para operar la entidad y también para ejercer sus responsabilidades de elaboración de informes financieros y de cumplimiento.

2.7.6. DOMINIOS

Los Dominios son definidos de la siguiente forma:

- **Planeamiento y Organización:** Este dominio cubre la estrategia y las tácticas y le concierne la identificación de la forma en que la tecnología de información puede contribuir mejor al logro de los objetivos del negocio. Más aún, la realización de la visión estratégica necesita planearse, comunicarse y administrarse desde diferentes perspectivas. Finalmente, debe instalarse una organización apropiada así como una infraestructura tecnológica.

- **Adquisición e Implementación:** Para comprender la estrategia de tecnología de información, las soluciones necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en el proceso del negocio. Además, se cubren en este dominio los cambios en y el mantenimiento de los sistemas existentes.
- **Entrega y Soporte:** A este dominio le concierne la entrega real de los servicios requeridos, que cubre desde las operaciones tradicionales sobre aspectos de seguridad y continuidad hasta el entrenamiento. Para brindar servicios deben instalarse los procesos de soporte necesarios. Este dominio incluye el procesamiento real de los datos por los sistemas de aplicación, a menudo clasificados como controles de las aplicaciones.
- **Monitoreo:** Todos los procesos de tecnología de información necesitan ser evaluados regularmente en el tiempo, en su calidad y cumplimiento con los requerimientos de control.

2.8. NORMATIVIDAD LEGAL VIGENTE EN EL PERÚ

El estudio detallado de la normatividad legal vigente en el país respecto al uso de tecnologías de la información, es de interés para los fines del presente trabajo de investigación. Por ello se hace referencia al compendio elaborado por el INEI y se trata en detalle las normas emanadas por la Contraloría General de la República y las orientaciones del INEI para entidades públicas.

2.8.1. COMPENDIO DE NORMATIVIDAD SOBRE EL USO DE TECNOLOGÍAS DE INFORMACIÓN EN EL PERÚ

El Instituto Nacional de Estadística e Informática del Perú[22] 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

[22] INEI. Compendio de Normatividad sobre el uso de Tecnologías de Información en el Perú. Pág. 1-299.

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.

A continuación se presenta la abstracción de dicho compendio.

I. Constitución Política del Perú

- Título I: De la persona y la sociedad. Art° 2
- Título V: De las Garantías Constitucionales. Art° 200

II. Norma que Grantiza la Libertad de Información

Ley N° 26301 Acción Constitucional de Habeas Data

III. Normas de Protección al Derecho de Autor

- Decreto Legislativo N° 822 Ley Sobre el Derecho de Autor (Protección Jurídica del Software)
- Decisión N° 351 Regimen Común sobre Derecho de Autor y Derechos Conexos
- Resolución N°0121-1998/ODA-INDECOPI Aprueban lineamientos de la Oficina de Derechos de Autor sobre uso legal de los programas de ordenador (Software)

IV. Normas sobre Delitos Informáticos

- Código Penal.
- Ley N° 27309 Ley que incorpora los Delitos Informáticos al Código Penal

V. Normas de Firma y Certificados Digitales

- Ley N° 27269 Ley de Firmas y Certificados Digitales

- Resolución Suprema N° 098-2000-JUS Designan Comisión Multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales
- Resolución Ministerial N° 074-2000-ITINCI-DM Designan representante del Ministerio ante la Comisión Multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales.
- Resolución Ministerial N° 276-2000-MTC-15.01 Designan representante del Ministerio ante la Comisión Multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales.
- Resolución Jefatural N° 021-2001-INEI. Designan representante ante el Consejo Superior de Fedatarios Juramentados con Especialización en Informática.
- Ley N° 27310 Ley que modifica el Art° 11 de la Ley N° 27269

VI. Normas que permiten la utilización de los medios electrónicos para la comunicación para la manifestación de voluntad

Ley N° 27291 Ley que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la voluntad.

VII. Normas que regulan el uso de las Tecnologías de la Información en la Gestión de Archivos y Documentos

- Decreto Legislativo N° 681 Normas que regulan el uso de Tecnologías Avanzadas en materia de Archivo de Documentos e Información en Computadoras
- Decreto Supremo N° 009-92-JUS- Aprueban el Reglamento del decreto Legislativo N° 681 sobre uso de Tecnologías de Avanzada en Materia de Archivo de las Empresas.
- Decreto Ley N° 25661 Comprenden a la Banca Estatal de Fomento, dentro de los alcances del Decreto legislativo N° 681 en cuanto al uso de

las tecnologías de microformas, microduplicados, micrograbación y otros análogos.

- CIRCULAR N° B-1922-92-SBS
- Circular Referida a la sustitución de archivos, mediante microformas y plazos de conservación de libros y demás documentos
- RESOLUCION N° 090-93-EF-94.10.0-CONASEV Dictan normas que permitan poner en práctica el uso de tecnologías avanzadas en materia de archivo de documentos
- LEY N° 26612
- Ley que Modifica el D. Leg. N° 681, Mediante el cual se Regula el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información
- DECRETO LEGISLATIVO N° 827 Amplían los Alcances del D. Leg. N° 681 a las Entidades Públicas a fin de Modernizar el Sistema de Archivos Oficiales
- DECRETO SUPREMO N° 002-98-ITINCI Aprueban Requisitos y Procedimiento para Otorgamiento de Certificado de Idoneidad Técnica para la Confección de Microformas
- DECRETO SUPREMO N° 001-2000-JUS Aprueban el Reglamento sobre la Aplicación de Normas que Regulan el Uso de Tecnologías Avanzadas en Materia de Archivo de Documentos e Información a Entidades Públicas y Privadas
- RESOLUCION MINISTERIAL N° 169-2000-JUS Aprueban Reglamento para supervisión de eventos de capacitación, conducentes al otorgamiento de certificado de idoneidad técnica de fedatario juramentado con especialidad en Informática
- LEY N° 27323 Ley que modifica el Decreto Ley N° 26126 - Ley Orgánica de Conasev, el Decreto Legislativo N° 604 - Ley de

Organización y Funciones del Instituto Nacional de Estadística e Informática, el Decreto Legislativo N° 681 - normas que regulan el uso

- de tecnologías avanzadas en materia de archivo y documentos y el Decreto Legislativo N° 861 - Ley del Mercado de Valores

VIII. Norma que Fomentan el Uso de los Formatos Electrónicos en las Entidades de la Administración Pública

- DECRETO LEGISLATIVO N° 809 LEY GENERAL DE ADUANAS
- DECRETO SUPREMO N° 121-96-EF REGLAMENTO DE LA LEY GENERAL DE ADUANAS
- RESOLUCION DE INTENDENCIA NACIONAL DE ADUANAS N° 000 ADT/2000-000750 Aprueban formatos e instructivos de la Declaración Unica de Aduanas (DUA) y la Orden de Embarque
- RESOLUCION DE INTENDENCIA NACIONAL N° 000 ADT-2000-001272 Prorrogan entrada en vigencia de resolución que aprueba formatos e instructivos de la Declaración Unica de Aduanas (DUA) y la Orden de Embarque
- RESOLUCION DE INTENDENCIA NACIONAL DE SISTEMAS N° 001-2000-ADUANAS Estructura de datos de la "DECLARACION UNICA DE ADUANAS - ELECTRONICA" (e-DUA), la "ORDEN DE EMBARQUE" y demás documentos del despacho aduanero electrónico
- RESOLUCION DE INTENDENCIA NACIONAL N° 000 ADT-2000-002180 Aprueban los instructivos de trabajo Declaración Unica de Aduanas (DUA) y Orden de Embarque O/E)
- RESOLUCION DE INTENDENCIA NACIONAL DE ADUANAS N° 000 ADT-2000-002797 Modifican el Instructivo de Trabajo "Declaración Unica de ADUANAS (DUA) INTA-IT.00.04"
- RESOLUCION DE SUPERINTENDENCIA DE ADUANAS N° 000103 Establecen a nivel nacional uso obligatorio del "Formato Electrónico de

Documentos Internos" (FEDI) en la tramitación interna de documentos que no estén relacionados con el despacho de mercancías

- RESOLUCION DE INTENDENCIA NACIONAL Nº 000 ADT/2001-000277 aprueban estructura de solicitudes electrónicas y modifican el procedimiento "autorización de operadores" inta-pe.00.08
- RESOLUCION DE SUPERINTENDENCIA Nº 002-2000/SUNAT (Publicada el 9 de enero del 2000) Dictan disposiciones referidas a la utilización de programas de declaración telemática para la presentación de declaraciones tributarias
- RESOLUCION DE SUPERINTENDENCIA Nº 044-2000/SUNAT (Publicada el 25 de marzo de 2000) Establecen disposiciones sobre declaración y pago de diversas obligaciones tributarias, mediante programas de declaración telemática
- RESOLUCION DEL SUPERINTENDENTE NACIONAL DE LOS REGISTROS PUBLICOS Nº 124-97-SUNARP
- Ley Nº 27419 Ley Sobre Notificación por Correo Electrónico
- DECRETO SUPREMO Nº 012-2001-PCM Texto Unico Ordenado De La Ley De Contrataciones y Adquisiciones del Estado
- DECRETO SUPREMO Nº 013-2001-PCM Reglamento De La Ley De Contrataciones y Adquisiciones del Estado

2.8.2. 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.

Los titulares de cada entidad son responsables de establecer, mantener, revisar y actualizar la estructura de control interno, que debe estar en función a la naturaleza de sus actividades y volumen de operaciones, considerando en todo momento el costo-beneficio de los controles y procedimientos implantados.

Las normas de control interno se fundamentan en principios y prácticas de aceptación general, así como en aquellos criterios y fundamentos que con mayor amplitud se describen en el marco general de la estructura de control interno para el sector público.

Las Normas de Control Interno para el Sector Público tienen los siguientes objetivos:

- Servir de marco de referencia en materia de control interno para las prácticas y procedimientos administrativos y financieros
- Orientar la formulación de normas específicas para el funcionamiento de los procesos de gestión e información gerencial en las entidades públicas
- Proteger y conservar los recursos de la entidad asegurando que las operaciones se efectúen apropiadamente
- Controlar la efectividad y eficiencia de las operaciones realizadas y que estas se encuentren dentro de los programas y presupuestos autorizados
- Permitir la evaluación posterior de la efectividad, eficiencia y economía de las operaciones, a través de la auditoría interna o externa, reforzando el proceso de responsabilidad institucional
- Orientar y unificar la aplicación del control interno en las entidades públicas

Las normas de control interno para el sector público están agrupadas en áreas y subáreas. Las áreas de trabajo constituyen zonas donde se agrupan un conjunto de normas relacionadas con criterios afines. Dentro de estas áreas se han establecido

normas de control relacionadas con los sistemas computarizados o informáticos, las cuales se dirigen a promover la eficiencia en la organización, mantenimiento y seguridad de los sistemas computarizados que procesan la información, que requieren las entidades para el desarrollo de sus actividades.

Las normas de control interno para sistemas computarizados pertenecen a la categoría 500 de las Normas de Control Interno para el Sector Público. Los sistemas computarizados permiten a los usuarios ingresar a los documentos y programas en forma directa, ya sea a través de un microcomputador, conocido como computadora portátil o mediante terminales que se les denominan microcomputadoras en línea. Los controles internos que requieren los ambientes que emplean microcomputadoras son diversos y en general están referidos a los accesos, contraseñas, desarrollo y mantenimiento de sistemas, los mismos que contribuyen a brindar seguridad y confiabilidad al procesamiento de información.

Conforme surgen nuevas tecnologías, los usuarios emplean sistemas de cómputo cada vez más complejos, lo que incrementa las aplicaciones que manejan y, a su vez, aumenta el riesgo y plantea la necesidad de implementar nuevos controles internos.

Las normas de control interno describen los controles que son necesarios para la implementación del área informática y el plan de sistemas de información de la entidad, según su actividad y durante un período determinado, así como los controles de datos fuente, de operación y de salida que preservan el flujo de información, además de su integridad. Asimismo, tales normas desarrollan los controles requeridos para el mantenimiento de equipos de cómputo y medidas de seguridad para el software (programas de computación) y hardware (equipamiento informático), así como los aspectos de implementación del plan de contingencias de la entidad.

El contenido de las normas de control interno para sistemas computarizados es el siguiente:

500-01 Organización del área informática

La dirección debe establecer políticas para la organización adecuada del área de informática que permita cumplir sus actividades con eficiencia, contribuyendo al desarrollo de las operaciones de la entidad

500-02 Plan de sistemas de información

Toda entidad que disponga de un área de informática debe implementar un plan de sistemas de información con el objeto que prever que el desarrollo de sus actividades contribuya al logro de sus objetivos institucionales

500-03 Controles de datos fuente, de operación y de salida

Deben diseñarse controles con el propósito de salvaguardar los datos fuente de origen, operaciones de proceso y salida de información, con la finalidad de preservar la integridad de la información procesada por la entidad.

500-04 Mantenimiento de equipos de cómputo

La dirección de cada entidad debe establecer políticas respecto al mantenimiento de los equipos de computación que permitan optimiza su rendimiento

500-05 Seguridad de programas, de datos y equipos de cómputo

Deben establecerse mecanismos de seguridad en los programas y datos del sistema para proteger la información procesada por la entidad, garantizando su integridad y exactitud, así como respecto de los equipos de computación

500-06 Plan de contingencias

El Area de Informática debe elaborar el Plan de Contingencia de la entidad que establezca los procedimientos a utilizarse para evitar interrupciones en la operación de sistema de cómputo

500-07 Aplicación de técnicas de Intranet

La implementación de las técnicas de Intranet dentro de las entidades debe efectuarse con el objeto de fortalecer el control interno e incrementar la eficiencia de las comunicaciones internas, previa evaluación del costo-beneficio que reportaría su aplicación

500-08 Gestión óptima de software adquirido a medida por entidades públicas

Debe establecerse políticas sobre el software a medida adquirido por las entidades, a fin que los derechos de propiedad se registren a nombre del Estado

2.8.3. RECOMENDACIONES TECNICAS PARA LA ORGANIZACION Y GESTION DE LOS SERVICIOS INFORMATICOS PARA LA ADMINISTRACION PUBLICA. DIRECTIVA Nº 010-95-INEI/SJI

Esta Directiva aprobada mediante RESOLUCIÓN JEFATURAL Nº 140-95-INEI, con fecha 8 de junio de 1995, tiene por finalidad brindar las recomendaciones técnicas y funcionales que deberán tenerse en cuenta para una adecuada organización, administración y evaluación de los Servicios Informáticos en la administración pública.

2.8.3.1. OBJETIVOS

- Orientar la adecuada organización de los Servicios Informáticos en las instituciones públicas que no disponen de este tipo de servicio.
- Dar pautas para la mejor gestión de un Servicio Informático, en las instituciones que ya disponen de este tipo de servicio.
- Establecer criterios de evaluación de un Servicio Informático.

2.8.3.2. BASE LEGAL

- Decreto Legislativo N° 604, Ley Organización y Funciones del INEI.
- Decreto Supremo N° 018-91-PCM, Reglamento de Organización y Funciones del INEI

Mientras que el alcance de la presente Directiva comprende a las dependencias encargadas de la organización o gestión de los servicios informáticos y a todo el personal que hace uso de equipos de cómputo en las entidades de la Administración Pública.

Aquí mencionaremos los aspectos principales que regulan la presente Directiva, mientras que en el anexo se adjunta completamente.

2.8.3.3. DE LA GESTIÓN TÉCNICA DE UN SERVICIO INFORMÁTICO

Los tipos o formas de brindar un Servicio Informático, son los siguientes:

a. Centros de Cómputo
b. Unidades de Cómputo de usuarios
c. Usuarios que disponen de computadora

Son funciones de un Servicio Informático las siguientes

- Dirección, Planeamiento Informático
- Desarrollo
- Soporte
- Producción
- Apoyo y asesoramiento a usuarios
- Capacitación
- Evaluación
- Control
- Elaborar el Plan Estratégico de Sistemas de Información o Plan de Sistemas

2.8.3.4. DE LA ORGANIZACIÓN DE UN SERVICIO INFORMÁTICO

a. Para crear un servicio Informático se deberá tener en cuenta lo siguiente:

- Conformar una Comisión Técnica al más alto nivel
- La Comisión Técnica elaborará un estudio de factibilidad
- La Comisión Técnica elaborará y/o contratará los servicios de terceros, para la elaboración de un Plan Estratégico de Sistemas de Información o Plan de Sistemas
- Institucionalizar el servicio en el organigrama funcional de la Institución

b. Para adecuar el Servicio Informático actual a las presentes Recomendaciones Técnicas

- Conformar una Comisión Técnica para la evaluación del Servicio Informático
- El desarrollo del Plan Estratégico de Sistemas de Información o Plan de Sistemas
- Evaluar el nivel o etapa de desarrollo alcanzado en la actualidad.
- La dirección del Servicio Informático implementará los planes de acción y normatividad necesarios para orientar un adecuado servicio.
- Racionalizar el uso de los equipos y aplicaciones de cómputo.
- El centro de Cómputo, incorporará al Plan de Trabajo Anual, un programa permanente de capacitación orientado a usuarios y a personal informático

c. La estructura interna del Servicio de Informática, presentará las siguientes características:

- Las funciones del servicio están reflejadas en el organigrama.
- El Centro de Cómputo dependerá orgánicamente de la Alta Dirección de la Institución

- La distribución de la funciones dependerá del tamaño del servicio de informática y de la filosofía de organización adoptada.
- Las funciones de desarrollo y de operación/soporte están siempre separadas.
- En caso de existir Unidades de Cómputo de Usuario y Usuarios con equipos de Cómputo, se establecerá un departamento de coordinación y apoyo a estas unidades y a los usuarios.

2.8.3.5. DE LA EVALUACIÓN DE LAS ACTIVIDADES INFORMÁTICAS

- El desarrollo de un Servicio Informático debe atravesar por varios estadios o etapas. En el anexo se muestra completamente esta descripción.
- La Dirección del Servicio Informático deberá evaluar periódicamente el grado de desarrollo alcanzado, mediante el uso de técnicas apropiadas.

2.8.3.6. DE LAS PAUTAS USADAS PARA EVALUAR LA EFICIENCIA Y EFECTIVIDAD DE UN SERVICIO INFORMÁTICO.

- Nivel eficiencia
- Nivel de efectividad

CAPÍTULO III

DISEÑO DE LA METODOLOGÍA

3.1. CONCEPCIÓN DE LA PROPUESTA DE AUDITORÍA INFORMÁTICA

Según Alonso Hernández García[23], "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."

FIG.N° 6: Esquema del concepto clásico de Auditoria

De aquí se deduce la importancia de establecer una opinión objetiva, fundada en las evidencias encontradas, sobre las diferencias existentes entre el planteamiento del

[23] Hernández. García, Alonso. La Informática como Herramienta del Auditor Financiero Coautor de Auditoría Informática. Piattini. Pág. 4

funcionamiento de cualquier área a auditar y su ejecución real en la organización, y comunicarlas a las personas correspondientes.

La auditoría informática según la define J.J.Acha[24], "es un conjunto de procedimientos y técnicas para evaluar y controlar total o parcialmente un Sistema Informático, con el fin de proteger sus activos y recursos, verificar si sus actividades se desarrollan eficientemente y de acuerdo con la normativa informática y general existente en cada empresa y para conseguir la eficacia exigida en el marco de la organización correspondiente".

La tendencia hoy en día para la realización de auditorías informáticas se muestran en el siguiente gráfico, donde se propone la necesidad de auditar la gestión que realizan las instituciones públicas en el uso de tecnologías de información, con la finalidad de identificar riesgos en el uso de las mismas y controles que permitan gestionar y administrar los riesgos eficientemente.

Fig. nº 7 Tipos de auditoría informática

[24] Hernández García. Alonso. Log. Cit. Pág. 12

El papel de la auditoría informática se convierte en algo más que una clásica definición del auditor informático: "... el auditor informático es responsable para establecer los objetivos de control que reduzcan o eliminen la exposición al riesgo de control interno. Después que los objetivos de auditoría se hayan establecido, el auditor debe revisar los controles y evaluar los resultados de su revisión para determinar las áreas que requieren correcciones o mejoras".

Creo que el papel del auditor informático tiene que dejar de ser el de un profesional cuya única meta empresarial sea analizar el grado de implantación y cumplimiento del control interno. Las organizaciones están invirtiendo mucho dinero en sistemas de información, cada vez son más dependientes de ellos y no pueden permitirse el lujo de tener profesionales mediatizados por esquemas tradicionales, pero que hoy en día no los son a tenor de las necesidades empresariales.

Aunque de forma simplista se trata de identificar la seguridad informática a la seguridad lógica de los sistemas, nada está mas lejos de la realidad hoy en día, extendiéndose sus raíces a todos los aspectos que suponen riesgos, debido al extensivo uso de las tecnologías de la información en los procesos de negocio de las entidades públicas.

José María González Zubieta[25] en su escrito sobre Metodologías de Control Interno, Seguridad y Auditoría Informática; nos dice que el campo del auditor informático de finales del siglo XX está orientado a la determinación de riesgos informáticos debido al explosivo desarrollo tecnológico de esta época de la humanidad que nos ha tocado vivir. Además continúa mencionando lo siguiente; si se define a la seguridad de los sistemas de información como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso.

En el presente trabajo de investigación 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,

[25] Gonzales Zubieta, Log. Cit. Pág.49.

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.

El enfoque de auditoría informática descrito líneas arriba permite gestionar internamente a la institución los riesgos y controles durante el uso de tecnologías de información.

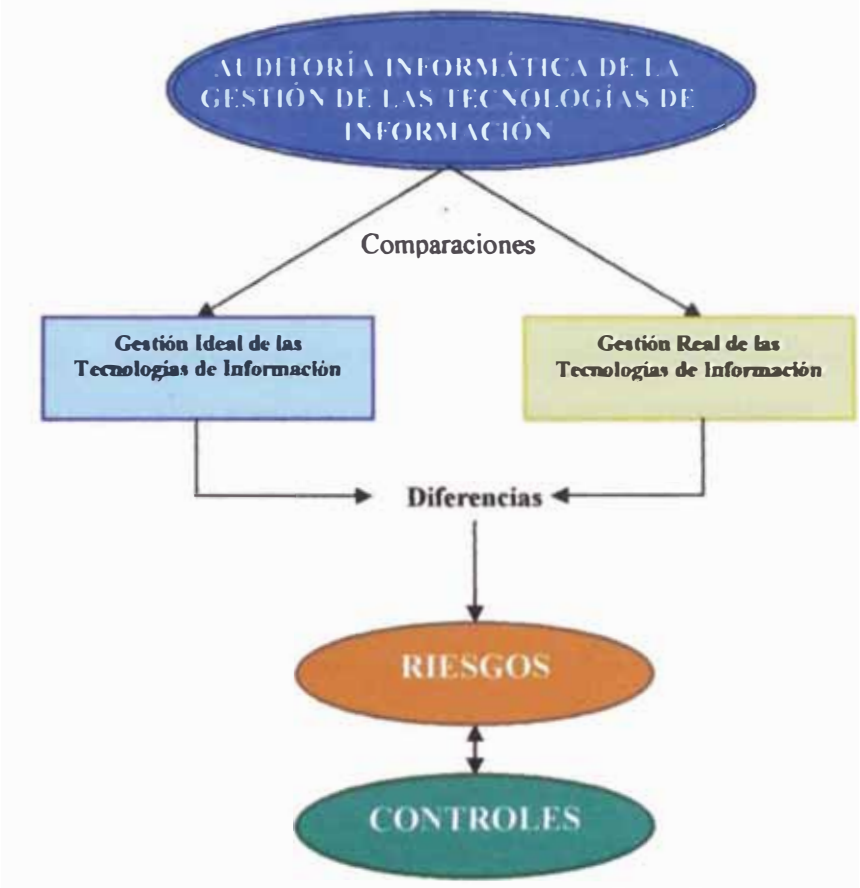


FIG. N° 8: esquema de la auditoria informática de la Gestión de Tecnologías de Información

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.

Con la finalidad de encontrar las mejores prácticas, que nos permitan eliminar los riesgos o implementar controles para reducirlos, se realizan procesos de benchmarking con normas, estándares o políticas probadas.

El COBIT, presenta normas de auditoría internacionalmente aceptada por las organizaciones dedicadas a la auditoría en el mundo, de allí la necesidad de conocerlas y aplicarlas a la metodología que se pretende implementar, puesto que presenta los Objetivos de control relacionados con la información y la tecnología

La estructura COBIT comienza con una premisa simple y pragmática: "Los recursos de tecnología de información necesitan ser administrados por un conjunto de procesos de tecnología agrupados naturalmente para proveer la información que necesita la empresa para el logro de sus objetivos".

Por otro lado contamos con la normatividad legal vigente en el Perú y orientado al uso de tecnologías de información en Entidades Públicas, entre ellas tenemos una serie de Leyes, Decretos, Normas; etc. Así mismos se cuenta con Normas Técnicas de Control Interno para el Sector Público, norma emanada por la Contraloría General de la República, por tanto de cumplimiento obligatorio en las entidades del estado y finalmente las recomendaciones técnicas del INEI para la gestión y organización de los servicios informáticos para la administración pública. Este conjunto de Normas legales, se deben utilizar tanto para la conceptualización del diseño metodológico, como para el diseño de cuestionarios.

De esta manera nace el concepto de evaluar e implementar las mejores prácticas para el uso de tecnologías de información emanadas por organismos legales y

estándares internacionales que permitan gestionar los riesgos y controles en el uso de las tecnologías de información en las instituciones públicas.

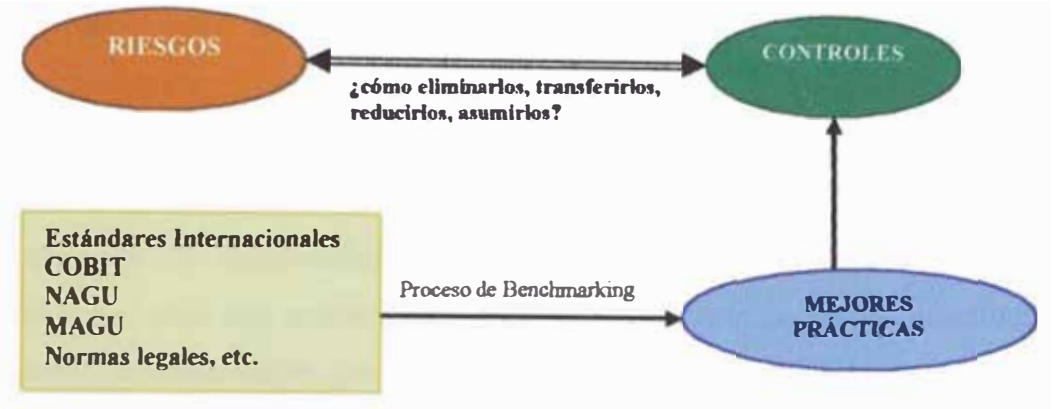


Fig N° 9 Esquema de Implementación de Controles

3.2. VISIÓN SISTÉMICA DE LA METODOLOGÍA PROPUESTA

La visón sistémica de la propuesta metodológica se muestra en el Gráfico N° 10, 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 de la Entidad que soporta una serie de procesos, que mantiene una cierta infraestructura tecnológica, que se administra en función a ciertos estándares de la Entidad, que para su funcionamiento realiza ciertos procedimientos, los mismos que pueden estar normados, que trabaja en equipo, sujeto al nivel de conocimientos en Tecnologías de Información del personal, etc. Es exactamente este entorno informático de la Entidad el que se va auditar.

El proceso de auditoría, muestra claramente dos áreas bien definidas: el Area de Riesgos y el Área de Control, los mismos que ya fueron explicados en los puntos anteriores, pero que aquí se muestran como dos áreas interdependientes, ya que el objetivo de la auditoría informática es la de proveer una revisión objetiva de los riesgos de la Entidad con relación al uso de tecnología de4 información y asegurar que están siendo controlados de una manera objetiva y eficiente. 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 en esta etapa del trabajo 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.

Este proceso de benchmarking es de suma importancia porque permitirá que las Entidades Públicas se gestiones con niveles de calidad internacionales.

Un proceso de Auditoría externa, si bien es cierto se realiza en un período de corte en el tiempo, debe servir para hacer el debido seguimiento a la implementación de las mejoras que se recomiendan. Por ello, el espíritu de la metodología propuesta es la guardar la información recolectada en la auditoría informática de manera que sirva efectivamente para realizar un seguimiento en el tiempo y para auditorías futuras; a la vez que pueda también servir para realizar procesos de benchmarking en otras Entidades Públicas con similares entornos tecnológicos.

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, como son: el avance acelerado de la tecnología, los costos de acceso a los mismos, la idiosincrasia propia que trae consigo la tecnología, los estándares internacionales, la competencia, el proceso de internacionalización, entre otros.

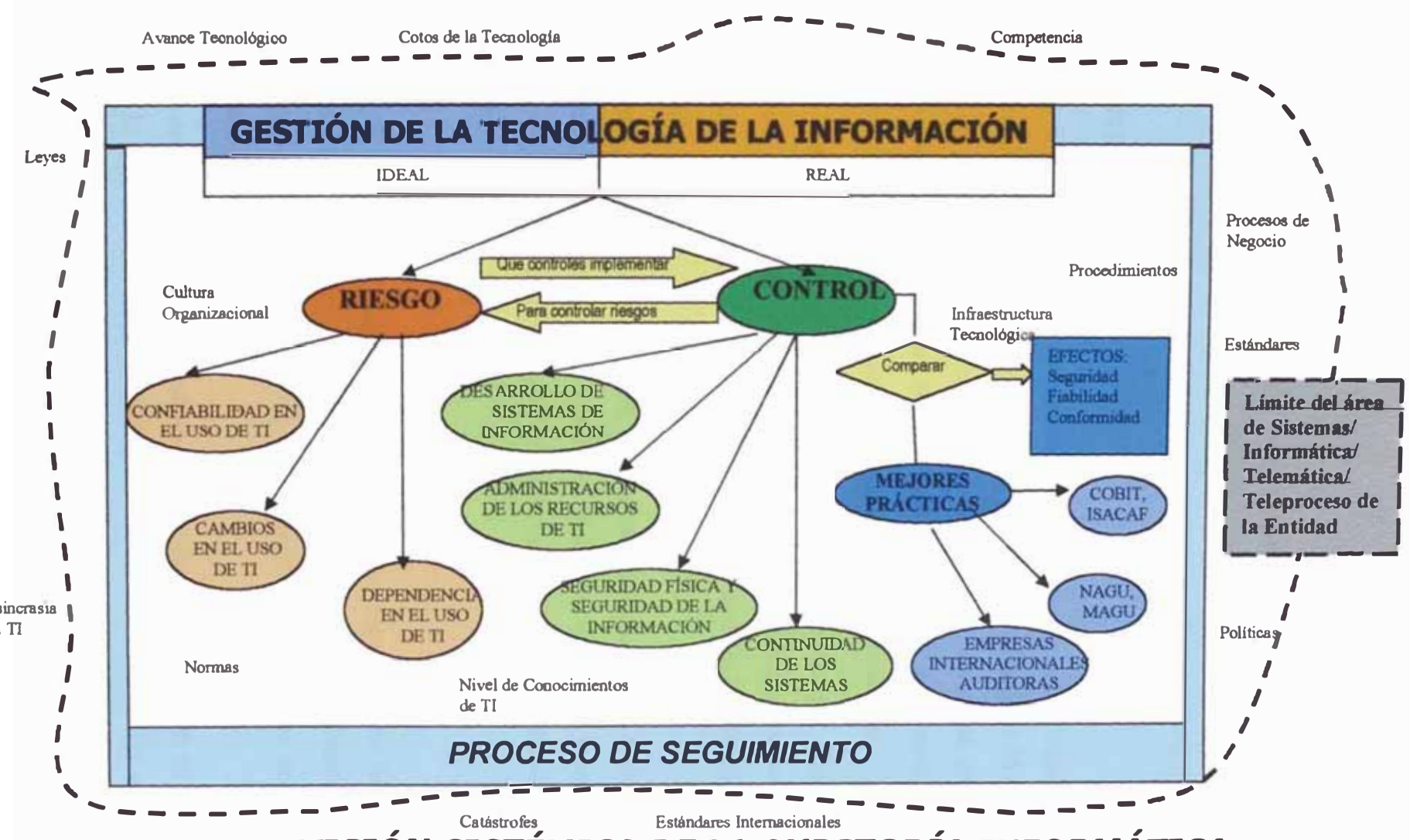


FIG. Nº 6: VISIÓN SISTÉMICA DE LA AUDITORÍA INFORMÁTICA

3.3. PRESENTACIÓN DE LA METODOLOGÍA DE AUDITORÍA INFORMÁTICA

3.3.1. ANTECEDENTES

Las Entidades Públicas son instituciones del Estado, están regidas por las Normas Técnicas de Control Interno para el Sector Público emitidas el 26 de junio de 1998, con la finalidad de optimizar sus sistemas administrativos, de gestión y de control interno. En estas normas se establece los criterios de control básicos a implementar con respecto al buen uso de la tecnología de información.

La estructura de control interno está conformada por las políticas, procedimientos, normas, directivas y otros lineamientos emitidos por las Entidades Públicas con la finalidad de proteger sus recursos materiales, personales, datos e información.

Para establecer una propuesta de modelo de metodología para el desarrollo de una Auditoria Informática para Entidades Públicas, debemos considerar los siguientes aspectos relacionados con la estructura de control interno que debe mantenerse:

a. Área de 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. Área de control. Un control establece las medidas implementadas en las Entidad con la finalidad de reducir los riesgos existentes y proteger los activos más importantes.

Debemos analizar los riesgos y controles más importantes que afectan a las Entidades Públicas, con la finalidad de relacionarlos con los aspectos de tecnología de información que se deben proteger, y formular nuestra propuesta de metodología.

3.3.2. DETERMINACIÓN DE LOS RIESGOS DE TECNOLOGÍA DE INFORMACIÓN A SER EVALUADOS

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

b. Confiabilidad en el uso de tecnología de información

c. Cambios en la Tecnología de Información

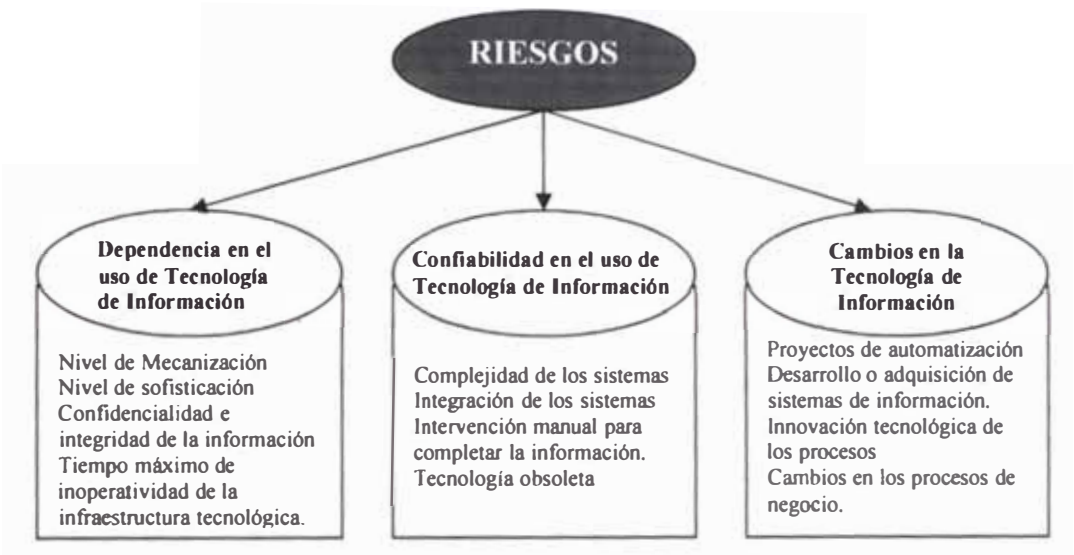


FIG. N° 11 Aspectos claves para la determinación de riesgos

A continuación analizaremos en detalle cada uno de las tres grandes áreas a evaluar en cuanto a riesgos:

a. Dependencia en el uso de tecnología de información

La dependencia en tecnología de información está relacionada con el uso que efectúa la Entidad y la importancia que representa para el desarrollo de sus operaciones. Se debe evaluar los siguientes factores:

- El nivel de mecanización de los procesos de negocio de la Entidad. Este nivel de mecanización nos indicará si se han elaborado sistemas de información para dar soporte a las áreas

usuarias ya sea administrativas en calidad de apoyo y a las de línea de acuerdo a la característica de cada Entidad.

- La sofisticación con respecto a la entrega de información en tiempo real y que influye en la toma de decisiones. Este factor nos permitirá determinar si la alta dirección o las áreas funcionales o áreas usuarias pueden tomar decisiones oportunas para informar a sus Entidades rectoras o para su propia toma de decisiones a fin de gestionar eficientemente la Entidad.
- La información que se genera en las áreas usuarias y la protección establecida considerando las normatividad vigente. Esta relacionado con la confidencialidad e integridad de la información que se utiliza para informar periódicamente a las instituciones rectoras o supervisoras de la Entidad.
- El tiempo que podría esperar la Entidad sin dar atención a los usuarios o clientes, a organismos reguladores; debido a la inoperatividad de su infraestructura tecnológica. Dicho tiempo puede ocasionar problemas en la toma de decisiones en la Entidad, que en algunos casos puede llegar a ser crucial o de importancia sumaria.

b. Confiabilidad en el uso de tecnología de información

La confiabilidad en el uso de tecnología de información está relacionada con resultados del procesamiento de datos y que no requieren trabajo manual por los usuarios para completar la información. Se debe evaluar los siguientes factores:

- La complejidad de los sistemas de información y el nivel de documentación existente. La complejidad está relacionada con algoritmos y cálculos especiales que realizan los sistemas para atender las necesidades de las áreas usuarias. Asimismo, se requiere documentar estos sistemas para hacerlos entendibles por otros usuarios.

- La integración de los sistemas de información y el uso de sistemas de información aislados por los usuarios. Esta relacionado con la generación de información incompleta de las áreas usuarias.
- Intervención manual para completar la información. Se relaciona con las actividades de los usuarios para preparar la información que requieren las áreas funcionales o gerenciales.
- Uso de sistemas de información de tecnología obsoleta. Se relaciona con el uso de sistemas no confiables en el procesamiento de datos al utilizar tecnología no vigente.

c. Cambios en la tecnología de información

Los cambios en la tecnología de información están relacionados 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. Se debe evaluar los siguientes factores:

- Principales proyectos de automatización. Los principales proyectos existentes indicarán la orientación hacia la cual desea llegar la Entidad en materia de eficiencia y eficacia operativa y de servicio.
- Desarrollo o adquisición de sistemas de información considerando las necesidades de automatización de la Entidad. Esta relacionado con la identificación de necesidades y evaluación de alternativas de solución.
- Uso de nueva tecnología de información en reemplazo de tecnología obsoleta recibida de gestiones anteriores. Esta relacionada con la innovación tecnológica en los procesos de negocio de la Entidad.
- Cambios a los procesos de negocio de la Entidad. Esta relacionado con la revisión de los procedimientos de trabajo y procesos de negocio para hacerlos mas eficientes y eficaces.

Los prototipos de encuesta a aplicarse en las instituciones públicas se muestran en los siguientes cuadros:

RIESGOS DEL AREA DE INFORMÁTICA

Cuadro N° 1	**Hoja N° _____ de _____**
Entidad: _____	**Año auditado: _____**
Auditor encargado: _____	**Fecha: _____/_____**
Auditor revisor: _____	**Fecha: _____/_____**

Evalúe lo siguiente	Exponga sus comentarios
Anote las implicancias para la auditoria de los siguientes riesgos y su relación con objetivos específicos de auditoria y la participación de especialistas. Factores de riesgos de TI a evaluar: • **Dependencia en TI** Evalúe: - El nivel de mecanización de los procesos de negocio de la Entidad. - La sofisticación con respecto a la entrega de información en tiempo real y que influye en la toma de decisiones. - La información que se genera en las áreas usuarias y la protección establecida considerando las normatividad vigente. - El tiempo que podría esperar la Entidad sin dar atención a los usuarios o clientes, a organismos reguladores; debido a la inoperatividad de su infraestructura tecnológica.	

Evalúe lo siguiente	Exponga sus comentarios
• **Confiabilidad en TI** Evalúe los siguientes factores: - La complejidad de los sistemas de información y el nivel de documentación existente. - La integración de los sistemas de información y el uso de sistemas de información aislados por los usuarios. - La Intervención manual para completar la información. - El uso de sistemas de información de tecnología obsoleta. • **Cambios en la tecnología de la Información:** Evalúe lo siguiente: - Los principales proyectos de automatización - El desarrollo o adquisición de sistemas de información considerando las necesidades de automatización de la Entidad. - El uso de nueva tecnología de información en reemplazo de tecnología obsoleta recibida de gestiones anteriores. - Los cambios a los procesos de negocio de la Entidad. (Anote que esto es alcanzado obteniendo un entendimiento del hardware, software y personal actual y planificado de la Entidad).	

3.3.3. IMPLEMENTACIÓN DE LOS CONTROLES DE TECNOLOGÍA DE INFORMACIÓN

Los controles de tecnología de información que la Entidad necesita implementar, consideran la minimización de los riesgos que pueden afectar el alcance de los objetivos de negocio establecidos.

Las áreas de control que la Entidad debe implementar se muestran en el siguiente gráfico.

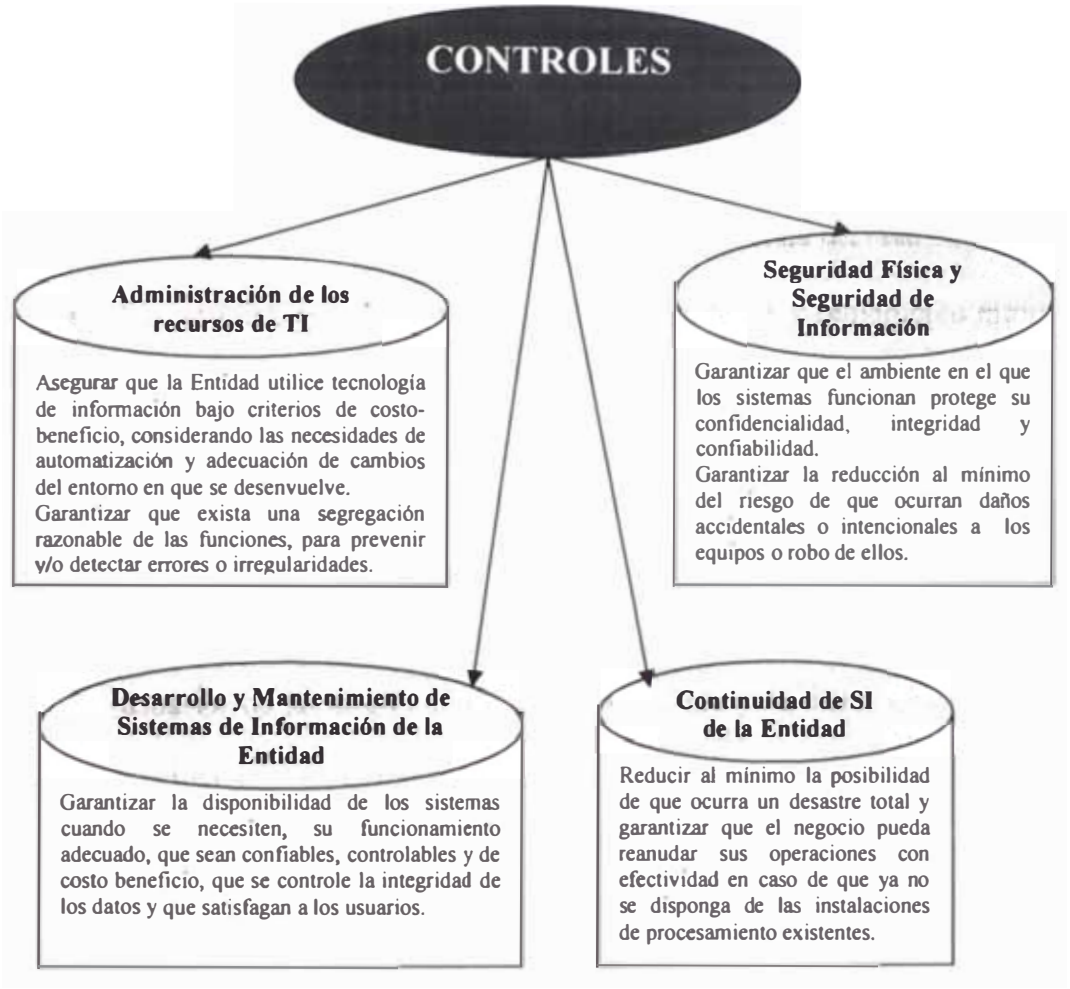


FIG. N° 12 Áreas de control según objetivos generales de auditoría.

A continuación describiremos cada una de las áreas de control que la Entidad debe implementar y detallaremos los aspectos involucrados en cada área,

con la finalidad de construir los prototipos que respondan a los objetivos generales y específicos definidos en esta etapa.

a. Administración de los recursos de tecnología de información

Esta área de control está relacionada con:

- La participación del encargado de sistemas o informática en el proceso de planeamiento de la Entidad y su aporte en aspectos de tecnología de información
- El proceso de planificación de los recursos de tecnología de información para los procesos administrativos, de gestión y de línea.
- La administración de los costos que representan la inversión en tecnología de información efectuado por la Entidad durante el año.
- El cumplimiento de la normatividad legal, leyes y reglamento interno de la Entidad, y su implementación en los sistemas de información
- La organización y nivel de reporte y comunicación del personal de sistemas o informática de la Entidad hacia la alta dirección y áreas funcionales.
- El uso de las facilidades de tecnología de información por parte de los usuarios de las áreas administrativas, gestión y de línea.

Para la evaluación de la administración de los recursos de información de la Entidad, se ha visto por conveniente evaluarlo a través de dos criterios complementarios y que se muestran en la Figura N° 13, la administración de los recursos en el área de sistemas y la segregación de funciones en el área de sistemas.

Cada una de estos criterios, a su vez se ha subdividido en aspectos específicos de evaluación y que también se incluyen en la Figura N° 13. A continuación se muestran los prototipos de cuestionario a aplicarse a las Entidades Públicas.

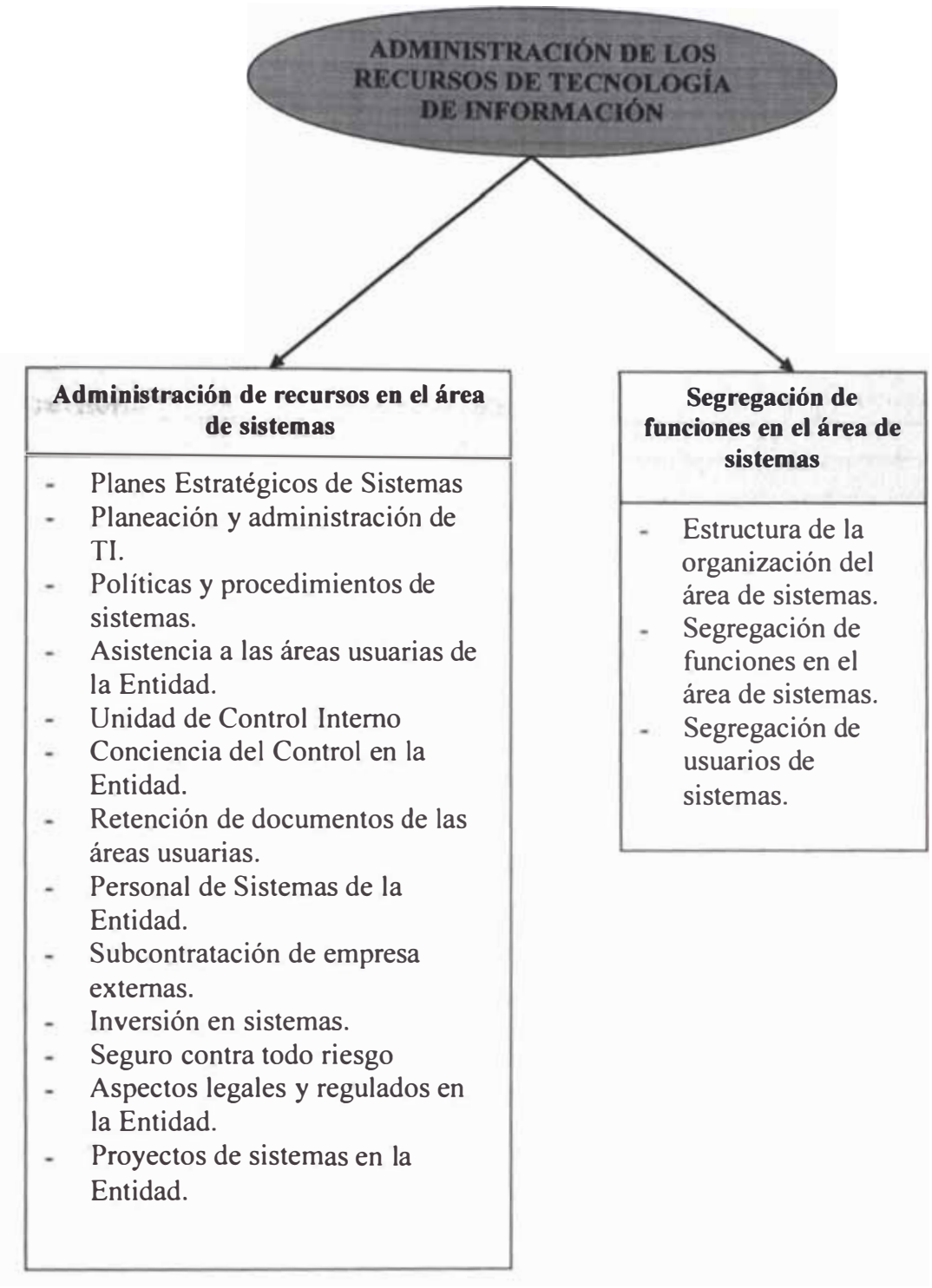


FIG. N° 13 Aspectos de control de la Administración de Recursos en el Area de Sistemas.

ADMINISTRACIÓN DE RECURSOS EN EL AREA DE SISTEMAS

Cuadro N°: 2 **Entidad:** _____ **Auditor encargado:** _____ **Auditor revisor:** _____	**Hoja N°:**_____ **de** _____ **Año auditado:** _____ **Fecha:** _____ **Fecha:** _____

Objetivo: **Asegurar que la Entidad utiliza tecnología de información bajo criterios de costo-beneficio, considera las necesidades de automatización y adecuación a cambios del entorno en que se desenvuelve.**	**Indique referencias**	**Exponga Comentarios**
Planes Estratégicos de Sistemas **1. Evalúe si la Entidad ha elaborado un Plan Estratégico de Sistemas, que determine la orientación para los próximos años.** **Evalúe lo siguiente:** • Que sea parte de la estrategia general de la Entidad • Que abarque todos los temas de la estrategia de la Entidad • Se encuentre actualizado y aprobado • Indique el nivel y calidad del personal involucrado • Haya sido aprobado por la Alta Dirección • Involucre el uso de tecnología emergente • Establezca el alcance, por ejemplo, áreas usuarias que participan.		

Administración de recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Planeación y Administración de TI 2. Evalúe si la Alta Dirección y otros funcionarios de la Entidad se involucran en temas relacionados con sistemas **Evalúe lo siguiente:** • El grado de participación de la Alta Dirección • Se realiza una revisión de las variaciones de costo-beneficio • Se preparan presupuestos destinados a la ejecución • Se tiene conformado un Comité de Sistemas • Existe comunicación formal de la estrategia de sistemas • Se tiene la representación de todas las áreas usuarias de la Entidad • Se haya establecido la periodicidad en la emisión de informes comparada con la estrategia diseñada • Los términos de referencia se encuentran aprobados		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Políticas y procedimientos de sistemas 3. Evalúe la existencia de políticas y procedimientos formales para administrar los recursos de sistemas **Evalúe lo siguiente:** • Que hayan sido aprobados por la Alta Dirección • Que establezca los objetivos de control, el alcance y la cobertura • Se hayan definido las responsabilidades • Se haya asignado la responsabilidad por el monitoreo o actualización • Haya sido distribuido al personal • Incluya asuntos con respecto a privacidad y derechos de autor. • Considere criterios de confidencialidad y seguridad de la información.		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Asistencia a las áreas usuarias de la Entidad 4. Evalúe si existe asistencia a los usuarios que laboran en la Entidad respecto al uso de los recursos de sistemas **Evalúe lo siguiente:** • La existencia de políticas y procedimientos con respecto a asistencia a usuarios • Se tiene control de las licencias de derechos de autor de los programas • Se mantiene en uso programas estándares • Existen procedimientos para combatir los virus • Se tienen controles de seguridad • Se ha distribuido al personal • Se utilizan generadores de informes		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Unidad de Control Interno 5. Evalúe si la Unidad de Control Interno de la Entidad participa activamente en los desarrollos y operaciones de sistemas. **Evalúe lo siguiente:** • Si se han elaborado los términos de referencia de la participación • Se ha preparado un organigrama formal • Existe independencia en los trabajos efectuados • El personal que participa tiene conocimiento de temas de sistemas • Se tiene entrenamiento o experiencia en sistemas • Existe cobertura y enfoque en las áreas de sistemas • La revisión de sistemas es integral • Acción que se toma sobre los hallazgos es oportuna		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Conciencia del Control en la Entidad 6. Evalúe si la actitud de la Alta Dirección de la Entidad propicia el control en las actividades efectuadas **Evalúe lo siguiente:** • Se realiza una evaluación del riesgo de sistemas informáticos • Se tiene en consideración asuntos de control en nuevos sistemas • Se manejan brechas en la seguridad • La responsabilidad sobre la seguridad ha sido asignada		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Protección de Información 7. Evalúe si la Entidad ha normado el uso y protección de información en medios seguros **Evalúe lo siguiente:** • El cumplimiento de la Entidad • El tipo y volumen de información protegida • Se establecieron requisitos futuros • Existen políticas establecidas por escrito		
Personal de Sistemas de la Entidad 8. Evalúe la existencia de políticas para contratar a personal de sistemas para laborar en la Entidad **Evalúe lo siguiente:** • La existencia de una política de contratación • La evaluación de experiencia y habilidades • Se otorga goce de vacaciones y horas extras • Se realizan evaluaciones de desempeño • Existen procedimientos de despido • Se provee entrenamiento de usuarios • Existe dependencia en personas claves • Se han establecido políticas y procedimientos de promoción de personal		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Subcontratación de empresas externas 9. Evalúe si la Entidad ha establecido procedimientos para administrar trabajos realizados por terceros **Evalúe lo siguiente:** • Existen acuerdos contractuales formales • Se evalúa el desempeño de acuerdo al servicio • Existen controles de seguridad • Existen cláusulas de confidencialidad • Se hace revisión de fijación de precios por el servicio • Existen nivel de dependencia y conocimiento de la junta directiva • Se realizan auditorias		
Inversión en sistemas 10. Evalúe si la Entidad ha preparado procedimientos que garanticen la inversión apropiada en sistemas **Evalúe lo siguiente:** • Existe una política para capitalizar / registrar los gastos • Existe un proceso de costeo formal • Se realiza revisión con los cambios y desembolsos que se anticipen • Se han considerado los cambios potenciales • Se ha evaluado el impacto de nueva tecnologíá		

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Seguro contra todo riesgo 11. Evalúe si la principal infraestructura de cómputo se encuentra protegida **Evalúe lo siguiente:** • Se han incluido todos los equipos de cómputo de la Entidad • Se ha considerado los casos de pérdida de utilidades e incremento del costo del trabajo • Se han considerado los costos de recuperación • Fraude / confidencialidad • Requisitos de seguro sobre el negocio (o sea, estipulaciones de la póliza)		
Aspectos legales y regulados en la Entidad 12. Evalúe si la Entidad ha preparado procedimientos para cumplir con las regulaciones propias de su entorno de desarrollo institucional **Evalúe lo siguiente:** • Existencia de requisitos fiscales o normativos • Existencia de requisitos de privacidad • Cumplimiento de derechos de autor • Otras regulaciones • Evidencia de cumplimiento		
Proyectos de Sistemas en la Entidad 13. Evalúe lo siguiente: • Verifique el uso de una metodología de administración de proyectos • Revise las políticas y procedimientos • Documente las técnicas de planeación • Revise el control del proyecto		

SEGREGACIÓN DE FUNCIONES EN EL AREA DE SISTEMAS

Cuadro Nº 3 **Entidad:** _____ **Auditor encargado:** _____ **Auditor revisor:** _____	**Hoja N°** _____ **de** _____ **Año auditado:** _____ **Fecha:** _____ **Fecha:** _____	
Objetivo: Garantizar que exista una segregación razonable de las funciones del personal, tanto dentro del Área de Sistemas como entre las funciones de sistemas y de los usuarios, para prevenir y/o detectar errores o irregularidades.	**Indique referencias**	**Exponga Comentarios**
Estructura de la Organización del Área de Sistemas 1. Evalúe la estructura de la organización de Área de Sistemas **Evalúe lo siguiente:** • El nivel de reporte de los informes del Área de Sistemas • El tamaño de las operaciones en comparación con las necesidades de la Entidad		

Segregación de Funciones en el Área de Sistemas	Indique referencias	Exponga Comentarios
Segregación de Funciones–Sistemas 2. Evalúe la segregación de funciones dentro del Área de Sistemas de la Entidad, considerando su tamaño de organización. **Evalúe lo siguiente:** • Analice la segregación de funciones, por ejemplo:. - Número de miembros del personal de sistemas - Programadores de sistemas - Programadores de aplicaciones - Administración de la base de datos - Operaciones de TI - Ingreso de datos - Operaciones de redes - Seguridad • Analice la confiabilidad en el personal clave • Analice la confiabilidad en el personal bajo contrato • Determine la segregación de la administración de usuarios		

Segregación de Funciones en el Área de Sistemas	Indique referencias	Exponga Comentarios
Segregación de Usuarios/Sistemas 3. Evalúe la limitación de responsabilidades de personal del Área de Sistemas de la Entidad **Evalúe lo siguiente:** • Analice la segregación de la administración de usuarios • Evalúe el acceso a contraseñas maestras • Determine la responsabilidad de iniciar o autorizar transacciones • Determine la custodia de los activos valiosos o móviles • Evalúe las modificaciones a los archivos maestros y otros datos • Analice la corrección de los errores en los datos de ingreso • Analice las pistas y revisión de auditoria		

b. Seguridad Física y Seguridad de Información

Esta área de control está relacionada con:

- El control de acceso a áreas restringidas dentro de la Entidad donde se han instalado los principales equipos de cómputo y equipos de comunicaciones que sirven para interconectar las diferentes áreas funcionales, gerenciales y operativas.
- Las medidas de protección establecidas en los ambientes destinados a las oficinas de sistemas o informática de la Entidad.
- La política de seguridad de información de la Entidad y su difusión entre las áreas gerenciales, funcionales y operativas.
- Las actividades de administración y monitoreo de la seguridad de información en las áreas funcionales, gerenciales y operativas
- Los controles de acceso a las redes y sistemas de información de la Entidad por los usuarios de las gerenciales, funcionales y operativas.
- La protección de las comunicaciones efectuadas con otras Instituciones o Entidades reguladoras

Para la evaluación de la seguridad física y seguridad de información de la Entidad, se ha visto por conveniente evaluarlo a través de dos criterios complementarios y que se muestran en la Figura N° 14, la seguridad de información en la Entidad y el control de acceso físico al área de sistemas.

Cada una de estos criterios, a su vez se ha subdividido en aspectos específicos de evaluación y que también se incluyen en la Figura N° 14. A continuación se muestran los prototipos de cuestionario a aplicarse a las Entidades Públicas.

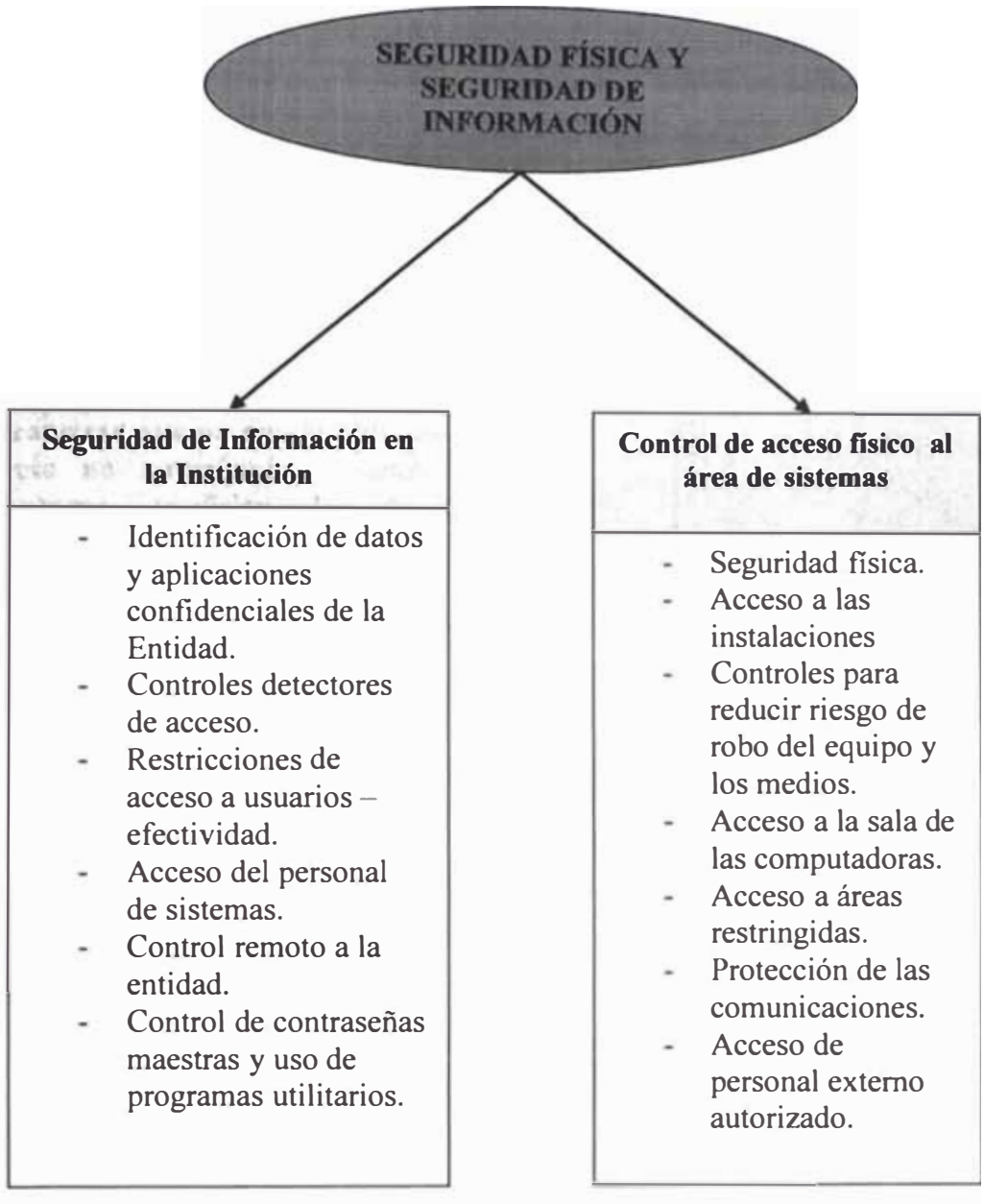


FIG. N° 14 Aspectos de control de la Administración de Recursos en el Área de Sistemas.

SEGURIDAD DE INFORMACIÓN EN LA INSTITUCIÓN

Cuadro N° 4 **Entidad:** _____ **Auditor encargado:** _____ **Auditor revisor:** _____	**Hoja N°** _____ **de** _____ **Año auditado:** _____ **Fecha:** _____ **Fecha:** _____

Objetivo: • **Garantizar que no pueda obtenerse acceso no autorizado a datos o programas confidenciales de la Entidad.** • Garantizar que el ambiente en el que los sistemas funcionan protege su confidencialidad, integridad y confiabilidad.	**Indique referencias**	**Exponga Comentarios**
Identificación de datos y aplicaciones confidenciales de la Entidad 1. Evalúe los procedimientos de la Entidad para proteger los datos y aplicaciones confidenciales **Evalúe lo siguiente:** • La existencia de una política de seguridad • La revisión de datos críticos durante el desarrollo • El proceso de evaluación de riesgos • El sistema de clasificación de datos		

Seguridad de Información en la Institución	Indique referencias	Exponga Comentarios
Controles Detectores de Acceso 2. Evalúe los controles para identificar los accesos no autorizados y potenciales problemas de seguridad y hacer un seguimiento adecuado? **Evalúe lo siguiente:** • El monitoreo y vigilancia de los registros • Que el propietario de los datos compruebe regularmente los usuarios activos y los derechos de acceso de los usuarios		
Restricciones del Acceso a Usuarios – efectividad 3. Evalúe las medidas de seguridad diseñadas por el Área de Sistemas. **Evalúe lo siguiente:** • Se realiza el cambio periódico de contraseñas • Se utiliza una longitud para las contraseñas • Existe protección de las contraseñas • Existen procedimientos de despido de personal con contraseñas de importancia • Se preparan informes sobre violaciones de seguridad		

Seguridad de Información en la Institución	Indique referencias	Exponga Comentarios
Acceso de personal de sistemas 4. Evalúe la existencia de controles que prevengan que el personal de sistemas acceda a los datos y programas de ambiente de producción. **Evalúe lo siguiente:** • Existen ambientes separados para producción y pruebas • Existen procedimientos para cambios de emergencia, - documentación actualizada - revisión periódica		
Acceso Remoto a la Entidad 5. Evalúe los procedimientos de la Entidad para otorgar acceso remoto a otras instituciones públicas. Evalúe lo siguiente: • Existe control de acceso remoto por proveedores de servicio • Existe control de acceso remoto de los usuarios • Existe control de acceso remoto del personal de sistemas		
Control sobre contraseñas maestras y uso de programas utilitarios 6. Evalúe si se tiene control de la asignación, autorización y uso de identificaciones o contraseñas maestras **Evalúe lo siguiente:** • Número de personas que tienen acceso • Nivel de acceso de los usuarios • Controles de protección compensatorios (ejm., controles de acceso) • Emisión de informes sobre las actividades		

CONTROL DE ACCESO FÍSICO AL ÁREA DE SISTEMAS

Cuadro Nº 5 **Entidad:** _____ **Auditor encargado:** _____ **Auditor revisor:** _____	**Hoja Nº** _____ **de** _____ **Año auditado:** _____ **Fecha:** _____ **Fecha:** _____

Objetivo: **Garantizar la reducción al mínimo del riesgo de que ocurran daños accidentales o intencionales al equipo o los medios de computadoras, o el robo de ellos.**	**Indique referencias**	**Exponga Comentarios**
Seguridad Física 1. Evalúe si existe seguridad física adecuada con respecto al equipo de computadoras y los correspondientes datos, medios y documentación **Evalúe lo siguiente:** • Los edificios (incluso la protección de las terminales) • La sala de las computadoras • El equipo de comunicación • El almacenamiento a prueba de incendios para los medios magnéticos • La prevención o detección de incendios • El almacenamiento externo a la localidad • La protección ambiental • La continuidad de la electricidad • La protección de los cables de la red		

Control de Acceso Físico al Área de Sistemas	Indique referencias	Exponga Comentarios
Acceso a las instalaciones 2. Evalúe si existen medidas de control para garantizar que sólo los miembros del personal o los visitantes autorizados entren a las instalaciones **Evalúe lo siguiente:** • El requerimiento que el personal y los visitantes porten distintivos visibles de identificación • Los procedimientos que controlen la emisión de pases o distintivos a los visitantes • El requerir a los visitantes que estén acompañados de un miembro permanente del personal • Que el personal esté consciente de la seguridad, o sea, que confronten a los visitantes que no estén acompañados		
3. Evalúe si existen controles para reducir el riesgo de robo del equipo y los medios **Evalúe lo siguiente:** • La autoridad que se requiere para retirar equipo de las instalaciones • La instalación de códigos de barra en el equipo • Los equipos sensores • La revisión de portafolios, bolsas		

Control de Acceso Físico al Área de Sistemas	Indique referencias	Exponga Comentarios
Acceso a la sala de las computadoras 4. Evalúe si está restringido el acceso a los salones de las computadoras sólo a personas autorizadas Evalúe lo siguiente: • Un registro de visitantes (incluso ingenieros de sistemas, encargados de la limpieza, etc.) • El uso de equipos de control de acceso (ejm. tarjetas-clave) • Los controles para prevenir el uso erróneo del sistema de acceso por tarjeta - diferentes niveles de acceso - asignación de tarjetas - registro de infracciones - investigación de las infracciones • Las restricciones de acceso a diferentes áreas • El requisito de que los visitantes estén acompañados		
Acceso a áreas restringidas 5. Evalúe si está más restringido el acceso a áreas que sean especialmente sensibles, tal como el área de telecomunicaciones **Evalúe lo siguiente:** • Los procedimientos de autorización de acceso • El registro de acceso • La revisión del registro de acceso		

Control de Acceso Físico al Área de Sistemas	Indique referencias	Exponga Comentarios
Protección de las comunicaciones 6. Evalúe si existen controles para prevenir la pérdida o interrupción de las comunicaciones **Evalúe lo siguiente:** • Los canales seguros para los cables • El salón de Servidores y Centro de Comunicaciones está bajo llave		
Acceso de personal externo autorizado 7. Evalúe si está adecuadamente restringido el acceso de personal externo autorizado **Evalúe lo siguiente:** • Coordinar, autorizar y vigilar a los visitantes encargados de servicio y mantenimiento • Que el equipo de limpieza y el personal de servicio firme un registro al entrar y salir del edificio y las áreas de computadoras • Que se acompañe al equipo de limpieza / otros en el área de las computadoras		

c. Desarrollo y Mantenimiento de sistemas de información para la Entidad

Esta área de control está relacionada con:

- El uso de una metodología de desarrollo de sistemas para el ciclo de vida de desarrollo de sistemas dentro de la Entidad, el cual será utilizado por el personal de sistemas o informática
- La administración de los proyectos de automatización requeridos por la Entidad.
- La participación de los usuarios finales en el ciclo de vida de desarrollo de sistemas y su aprobación respectiva
- La administración de la calidad de los productos resultantes de los proyectos de automatización en la Entidad.
- La documentación de los sistemas de información a nivel técnico y de usuario.

Para la evaluación del desarrollo de sistemas se han tomado en cuenta los siguientes aspectos claves, que se muestran en la Figura Nº 15. A continuación se muestran los prototipos de cuestionario a aplicarse a las Entidades Públicas.

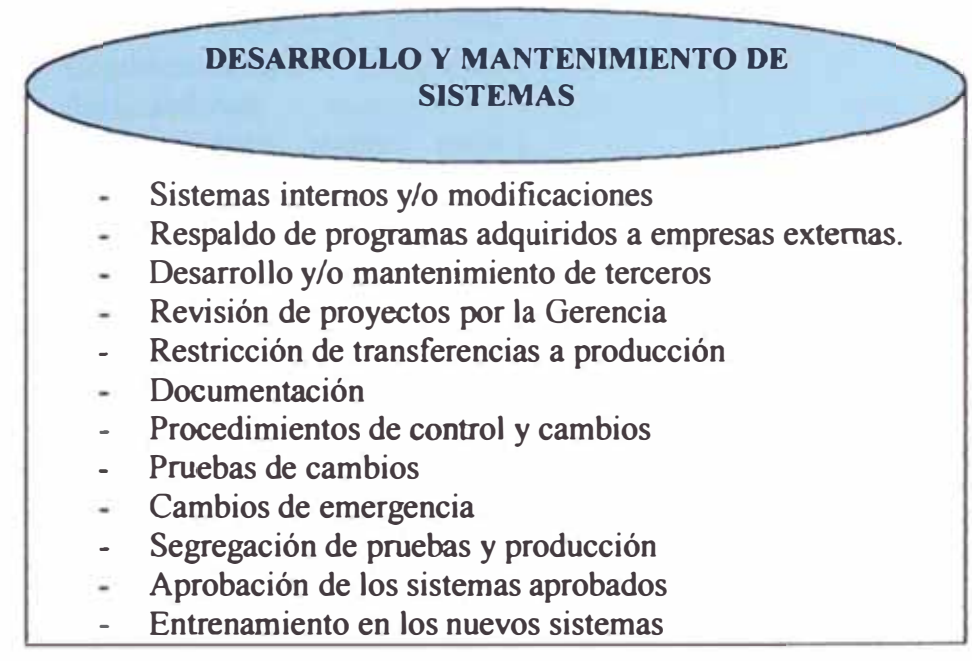


Fig. Nº 15 Aspectos de control del Desarrollo de Sistemas

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Cuadro Nº 6 **Entidad:** _____ **Auditor encargado:** _____ **Auditor revisor:** _____	**Hoja Nº** _____ **de** _____ **Año auditado:** _____ **Fecha:** _____ **Fecha:** _____	
Objetivo: Garantizar que los sistemas estén disponibles cuando se necesiten, que funcionen debidamente, que sean confiables, controlables y de costo beneficio, que tengan controles estrictos sobre la integridad de los datos y que satisfagan las necesidades de los usuarios	**Indique referencias**	**Exponga Comentarios**
Sistemas internos y/o modificaciones 1. Evalúe la metodología de desarrollo de sistemas utilizada por el Área de Sistemas. **Evalúe lo siguiente:** • Indique la metodología utilizada • Confidencialidad, integridad, disponibilidad, control y facilidad para auditar están incorporados en la metodología de desarrollo utilizada • Incluye procedimientos internos desarrollados por el equipo de desarrollo de sistemas • Se utilizan programas prototipos • Existen normas de programación		

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Respaldo de programas adquiridos a empresas externas 2. Evalúe si el personal de sistemas da mantenimiento continuo a los programas. **Evalúe lo siguiente:** • Existe un contrato de mantenimiento con el proveedor • Se realiza verificación y pruebas de los cambios y mejoras antes de su instalación • Se ha obtenido el código fuente • Se tienen medidas para prevenir el acceso no autorizado a los programas • En cuanto al proveedor de programas: cantidad de personal de respaldo, referencias, confiabilidad • Se tienen contratos actualizados • Se realiza certificación de los programas • Se evalúan las implicaciones de las modificaciones internas • Los sistemas de información son estables		
Desarrollo y/o mantenimiento de terceros 3. Evalúe los estudios de costo y beneficio de los trabajos realizados con el apoyo de empresas externas **Evalúe lo siguiente:** • Se tiene una administración de los costos • Se evalúa la reputación de proveedor • Se evalúa la calidad del personal • Se mantienen normas de programación • Existen antecedentes de la empresa		

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Revisión de Proyectos por la Gerencia 4. Evalúe si la Alta Dirección revisa los avances en los trabajos de desarrollo y cambio a los sistemas así como los costos relacionados. **Evalúe lo siguiente:** • La periodicidad de emisión de informes a la alta gerencia • El control de los presupuestos • Los métodos de costos • El monitoreo del proceso • Todos los costos sean incluidos		
Restricción de Transferencias a Producción 5. Evalúe la limitación para instalar nuevas versiones en el ambiente de producción. **Evalúe lo siguiente:** • Se mantiene controles de acceso • Que el personal de desarrollo no pueda trasladar los programas a producción • Se registran pistas de auditoria de los pases de programas		
Documentación 6. Evalúe la documentación de los sistemas de información. **Evalúe lo siguiente:** • Se mantiene una descripción de los objetivos de los sistemas • Se da cumplimiento de normas de programación • Se mantiene documentación del sistema • Existen instrucciones de operación • Existe documentación de usuarios		

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Procedimientos de Control de Cambios 7. Evalúe si se mantienen procedimientos apropiados para autorizar y documentar la iniciación y traslados a producción de los cambios. **Evalúe lo siguiente:** • Se tienen procedimientos para aprobar las solicitudes de los usuarios • Se tiene políticas de documentación • Se mantiene documentación de los cambios a los programas • Se requiere la autorización de la Jefatura • Se mantiene un registro de los cambios (generales y detallados) y antecedentes del programa		
Pruebas de Cambio 8. Evalúe la existencia de las pruebas de los cambios por los que los desarrollan y por los usuarios **Evalúe lo siguiente:** • Se tienen procedimientos de prueba • Se logra la participación de los usuarios en la autorización y la prueba de los cambios • Se obtienen pruebas completas y apropiadas • Se mantienen pruebas debidamente documentadas y analizadas		

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Cambios de Emergencia 9. Evalúe los procedimientos establecidos para controlar cualquier cambio de emergencia que efectúe el personal de desarrollo de sistemas **Evalúe lo siguiente:** • Se obtiene la aprobación del operador de sistemas • Se mantiene registro de todos los cambios de emergencia • Se realizan pruebas • Se obtiene la aprobación posterior de la Alta Dirección, del J • efe de Sistemas, según corresponda		
Segregación de Pruebas y Producción 10. Evalúe si se asignan bibliotecas por separado para las pruebas de desarrollo y las actividades de producción **Evalúe lo siguiente:** • Se mantiene una segregación de bibliotecas de desarrollo / pruebas de aceptación / producción • Se tienen procedimientos / restricciones de transferencias / traslados		
Aprobación de los sistemas probados 11. Evalúe si se requiere una aprobación formal después de efectuar pruebas del sistema. **Evalúe lo siguiente:** • La oportunidad de la aprobación (por ejemplo, antes de trasladar a producción) • La autoridad del individuo que efectúe la aprobación		

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Entrenamiento en los nuevos sistemas 12. Evalúe si reciben los usuarios un entrenamiento apropiado sobre las facilidades de los nuevos sistemas antes de la implantación. **Evalúe lo siguiente:** • Flujogramas del sistema • Diagramas de flujo de datos • Estructuras de datos lógicos • Diccionario de base de datos • Especificaciones del sistema • Especificaciones del programa • Almacenamiento externo de copias de la documentación esencial		

d. Continuidad de Sistemas de la Entidad

Esta área de control está relacionada con:

- Las medidas de protección ante la posibilidad de que ocurra un desastre en la Entidad.
- Las acciones a tomar para garantizar la continuidad de los sistemas de información de la Entidad.
- Determinación de las funciones y sistemas críticos de la Entidades.
- La existencia de planes de contingencia, con procedimientos claramente establecidos, métodos provisionales de trabvajo.
- La existencia de políticas y procedimientos de respaldo

Para la evaluación de la continuidad de los sistemas de la Entidad, se ha visto por conveniente evaluarlo a través de los siguientes criterios complementarios que se muestran en la Figura N° 16. Además a continuación se muestran los prototipos de cuestionario a aplicarse a las Entidades Públicas referidas al este último aspecto a auditar.

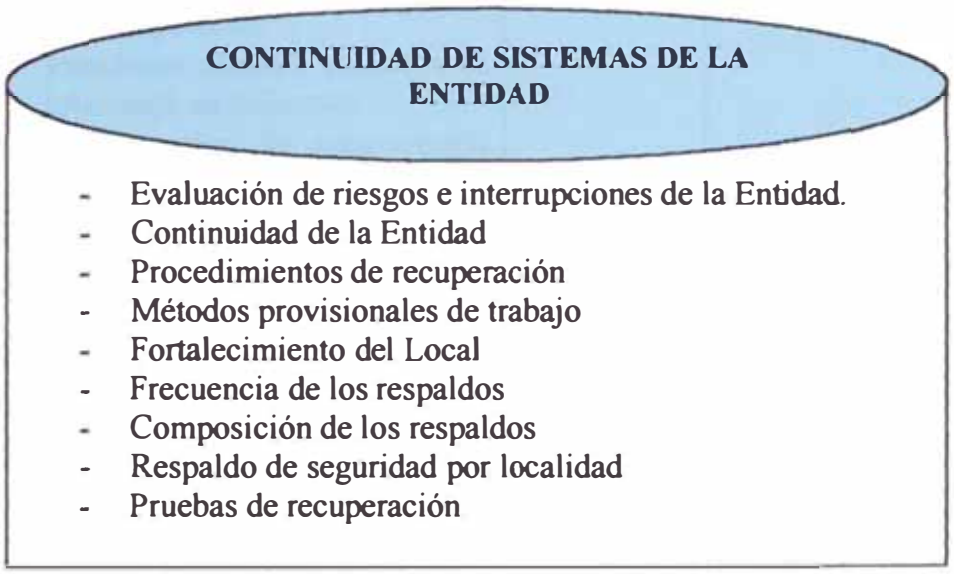


Fig. N° 16 Aspectos de control para la Continuidad de Sistemas.

CONTINUIDAD DE SISTEMAS DE LA ENTIDAD

Cuadro Nº 7 **Entidad:** _____ **Auditor encargado:** _____ **Auditor revisor:** _____	**Hoja Nº** _____ **de** _____ **Año auditado:** _____ **Fecha:** _____ **Fecha:** _____	
Objetivo: **Reducir al mínimo la posibilidad de que ocurra un desastre total y garantizar que el negocio pueda reanudar sus operaciones con efectividad (dentro de un período razonable de tiempo) en caso que ya no se disponga de las instalaciones de procesamiento existentes.**	**Indique referencias**	**Exponga Comentarios**
Evaluación de Riesgos–Interrupción de la Entidad 1. Evalúe si se han identificado las funciones y los sistemas críticos de la Entidad. **Evalúe lo siguiente:** • Funciones claves y períodos de tolerancia en cada caso • Que el plan de recuperación tome en cuenta los asuntos de negocio y de computadoras • Tiempo que el negocio funcionar con efectividad sin sus sistemas críticos de computadoras		

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Continuidad de la Entidad 2. Evalúe si se ha documentado un plan de continuidad del negocio que sea apropiado **Evalúe lo siguiente:** • Revisión y actualización periódica del plan • Procedimientos de los usuarios. • Aprobación de la Alta Dirección. • Alcance, de los sistemas centrales y computación de usuarios; servicios internos y de terceros; TI e ingreso de datos de los usuarios		
Procedimientos de recuperación 3. Evalúe si han especificado los usuarios sus requisitos de recuperación **Evalúe lo siguiente:** • Los niveles de interrupción • Recuperación de las aplicaciones críticas solamente • Recuperación de las aplicaciones • Procedimientos adicionales para el manejo del ingreso de datos, si fuese apropiado • Duración de los métodos provisionales de procesamiento		
Métodos de trabajo provisionales 4. Evalúe si han desarrollado los usuarios métodos de trabajo provisionales (como parte de sus procedimientos de recuperación) para ponerlos en práctica en caso que se interrumpa el procesamiento normal		

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Fortalecimiento del Local 5. Evalúe si se efectúan revisiones periódicas de los análisis de riesgo, como parte de un ejercicio para evitar desastres, para reducir al mínimo la posibilidad de que ocurra una interrupción total **Evalúe lo siguiente:** • El alcance de las revisiones • La fecha de la revisión más reciente • Las medidas tomadas		
Prevención y Reducción de Interrupciones 6. Evalúe si están los sistemas y las operaciones de negocios diseñados de una manera efectiva para reducir las interrupciones al mínimo **Evalúe lo siguiente:** • Protección contra intromisión no autorizada • Rutas alternas para las redes • Reemplazo de componentes • Respaldo ofrecido por los proveedores de los equipos • Mantenimiento preventivo		

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Frecuencia de los Respaldos 7. Evalúe si se hacen copias de respaldo de los archivos de datos y los programas y se almacenan dentro y fuera de la localidad con suficiente periodicidad **Evalúe lo siguiente:** • Oportunidad del respaldo • Frecuencia • Relación con el procesamiento / cambios críticos • Duración de los ciclos de los procesos principales • Volúmenes de datos comprarados con los respaldos almacenados externamente • Recuperabilidad de los documentos fuentes • Respaldos periódicos parciales comparados con respaldos completos		
Composición de los Respaldos 8. Evalúe si se respalda lo siguiente de manera apropiada: • Los archivos de datos • Los programas • Los programas de los sistemas • La documentación de los sistemas • Los procedimientos de operación • Los procedimientos de usuarios • Plan de Recuperación en Caso de Desastre		

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Respaldo de Seguridad / Localidad 9. Evalúe si se mantienen las copias de respaldo en una localidad segura tanto localmente como externa a donde se encuentran las computadoras **Evalúe lo siguiente:** • Registro de los traslados de los medios de almacenamiento • Autoridad para trasladar los medios • Lo apropiado de las localidades internas y externas de almacenamiento • Cómo se efectúan los respaldos para garantizar su recuperación		
Pruebas de Recuperación 10. Evalúe si se someten a pruebas apropiadas los procedimientos de respaldo y de recuperación **Evalúe lo siguiente:** • El tiempo que toma recuperar • El procesamiento involucrado en la recuperación • Las pruebas efectuadas después de cambios al sistema y a los programas • La frecuencia de las pruebas • La fecha y el resultado de la última prueba • La efectividad de las pruebas • Medidas posteriores adoptadas • Los cambios en los programas del sistema que puedan impactar la recuperación		

3.4. TÉCNICAS DE EVALUACIÓN

3.4.1. CUESTIONARIOS

Los cuestionarios son el instrumento evaluativo que más prefieren los auditores, debido a que resulta fácil identificar una serie de preguntas dirigidas a conocer el grado de vulnerabilidad del sistema de control interno de las empresas, así como para la identificación de riesgos.

El uso de esta técnica será confiable y útil para el seguimiento de las mejoras llevadas acabo por la Empresa, siempre que las respuestas que se recojan no sean del tipo cerradas; sino más bien abiertas y además que permitan recoger los aspectos que llevaron al Auditor a calificar un determinado item como de alto riesgo, sin riesgo o con riesgo presente. De tal manera que cuando se realice el seguimiento se evalúe si continúan presentes dichos aspectos o fueron eliminados, o de otro modo nos permitan guardar información respecto a las mejores prácticas de control encontradas en la auditoría cuando éstas fueron calificadas como sin riesgo, las mismas que servirán para implementarlas en otras organizaciones con similares entornos.

Este es el tipo de cuestionario que se presenta, a diferencia de los de respuesta cerrada, están altamente limitados a la concepción y nivel de conocimientos del auditor, quedando posteriormente inutilizable dichas respuetas para una siguiente auditoría e inclusive a cargo de otro auditor, quien no podrá entender ampliamente las causas que llevaron a su colega a calificar de una u otra manera un determinado aspecto de la auditoría.

La técnica de los cuestionarios sigue siendo válida para diagnosticar el sistema de control interno, pero amerita precisar, que los cuestionarios deben ser diseñados a la medida. Esto sugiere que el auditor estará frente a un nuevo reto, siempre que se ocupa de un nuevo trabajo de auditoría.

Los cuestionarios no deben copiarse o aplicarse como estándares. Es necesario que el auditor ponga a prueba su capacidad académica, experiencia, creatividad, etc. al servicio de cada auditoría diseñando cuestionarios a la medida. Esto hace además

que la auditoría no sea una actividad monótona, sino muy dinámica y exigente profesionalmente hablando.

3.4.2. ENTREVISTAS

La entrevista es una técnica complementaria de los cuestionarios para conocer el grado de vulnerabilidad de los sistemas de control. A los auditados les agrada más esta modalidad, especialmente cuando se aplica de manera informal. Es decir, cuando se maneja un diálogo profesional libre de tensiones y de circunstancias desfavorables para los resultados de la auditoría.

Por otra parte, en las entrevistas se pueden utilizar grabadoras, filmadoras, para facilitar la obtención de información.

3.4.3. ANÁLISIS DE DOCUMENTOS

Esta técnica consiste en que los auditados expresan por escrito sus responsabilidades, sus funciones y los procedimientos que siguen en las actividades de su trabajo. Como es evidente, esta técnica no es preferida por los auditores debido a los dispendioso para concluir los resultados, especialmente cuando se trata de numerosos auditados, por lo tanto nosotros lo utilizaremos durante el levantamiento de información con la finalidad de realizar el diagnóstico preliminar de la organización.

3.4.4. MODELOS MATRICIALES

Los modelos matriciales constituyen un instrumento muy valioso para analizar los riesgos y para establecer el grado de validez técnico del sistema de control. Se pueden idear numerosas matrices de control , colocando por el lado de las columnas los puntos de control o escenarios de riesgo y por el lado de las filas las amenazas o causas de riesgos potenciales.

Aquí el criterio del auditor juega un papel preponderante en el diseño de las matrices y sus modalidades de ponderación, debido a que en cada objeto auditable existen puntos de alto, medio y bajo nivel de criticidad.

3.5. ETAPAS PARA EL DESARROLLO DE LA AUDITORÍA INFORMÁTICA

La Auditoría Informática es un trabajo que se realiza en equipo y requiere de un proceso de planificación para su ejecución exitosa, a continuación se muestra las etapas que deben seguirse para el desarrollo de un trabajo de auditoría.

3.5.1. ENTENDIMIENTO DE LA ENTIDAD

Antes de realizar las etapas específicas de una auditoría informática, se debe cumplir con esta primera etapa correspondiente a lograr un entendimiento global de la Entidad a auditar, con la finalidad de conocer el sector al que pertenece, el giro de la organización, el entorno en el que se desenvuelve, cuáles son sus objetivos, sus estrategias; con la finalidad de evaluar si las Tecnologías y Sistemas de Información implementados, sirven de apoyo a la Entidad, si existen riesgos en el uso de los mismos o si están siendo efectivamente controlados.

Diferentes Tecnologías de Información sirven a propósitos específicos de negocio, de allí la importancia de conocer y entender en una primera etapa a la Entidad a auditar.

Para una mejor cobertura se ha sub-dividido esta etapa en los siguientes aspectos:

3.5.1.1. ENTENDIMIENTO ORGANIZACIONAL

Orientado a conocer y entender la visión, misión y cultura organizacional de la Entidad en el entorno en que se desenvuelve.

Conocer su historia y los fines para los cuales fue creado; en función a ello cómo se ha organizado la Entidad y cuál es el entorno en el que compite o se desarrolla.

Para cumplir con esta primera etapa utilizaremos la técnica del análisis documental, como son: análisis del organigrama, análisis del Manual de Organización y Funciones, la Normatividad legal que norma la vida institucional, entre otros. Por otro lado utilizaremos el análisis de la Cadena de Valor y el Análisis de las 5 Fuerzas Competitivas de Porter, para conocer a profundidad la razón de ser de la entidad, su entorno competitivo, las actividades primarias y de apoyo que permiten operativizar la Entidad.

A continuación es importante conocer sus objetivos estratégicos, los proyectos que desarrolla o pretende desarrollar, así como las metas y estrategias que le permitirán el logro de sus objetivos.

Este entendimiento permitirá al auditor informático evaluar en qué medida el uso o mal uso de las tecnologías de información ayudan o ponen en riesgo el logro de dichos objetivos.

3.5.1.2. PROCESOS DE NEGOCIO DE LA ENTIDAD

Es importante determinar los procesos de negocio más importantes que realiza la entidad y especialmente aquellos donde se encuentran involucrados el uso de tecnologías de la información.

Por tanto, se hará una descripción detallada de los procesos de negocio, para entender claramente a qué funciones apoyan y los procedimientos que siguen, nos ayudaremos de la Cadena de Valor en este aspecto.

3.5.1.3. INFRAESTRUCTURA TECNOLÓGICA DE LA ENTIDAD

Está orientada a determinar el tipo de tecnología que ha implementado la Entidad y los Sistemas de Información que maneja.

Para ello, es necesario identificar las LANs y WANs que pudieran existir, describiendo sus características más importantes, tales como: tecnología que usa, tipo de comunicación que utiliza, tamaño, alcance, plataforma sobre la que corre, etc.

De la misma manera es necesario conocer el Software Base que utiliza y los tipos de software de aplicación que maneja.

Obtener la arquitectura tecnológica permitirá entender mejor su actual implementación y sus planes de desarrollo informáticos.

3.5.1.4. DESCRIPCIÓN DEL ÁREA DE INFORMÁTICA

Es necesario brindarle una atención especial a ésta área, para conocer y entender su organización, su política, conocer la cantidad de personal que labora en dicha área, su nivel de capacitación y las funciones que tiene asignados. A fin de determinar el rol que desempeña en la gestión de las tecnologías de información en correspondencia con la normatividad legal vigente en el Perú.

3.5.1.5. DIAGNÓSTICO DE LA ORGANIZACIÓN

Para cumplir con esta etapa es importante conocer internamente a la Entidad y el entorno en que se desenvuelve, entender los riesgos que enfrenta en el actual mundo competitivo y donde no sólo las empresas privadas, sino también las Entidades Públicas tienen que mantener altos niveles de competitividad, lograr su acreditación en el sector donde se desarrolla, satisfacer las exigencias de sus usuarios y/o clientes, responder rápidamente a los cambios cada vez más veloces del entorno y lograr estándares internacionales de calidad de servicio.

Utilizaremos las siguientes herramientas de evaluación: Cadena de Valor, las 5 Fuerzas Competitivas de Porter, el análisis FODA y el análisis de Vulnerabilidad para obtener un diagnóstico organizacional completo.

3.5.2. DETERMINACIÓN DE LOS ALCANCES Y OBJETIVOS

Esta etapa es de suma importancia para iniciar el trabajo específico de auditoría informática, puesto que deben quedar explícitamente señalados los objetivos y alcance de la auditoría informática.

Esta etapa podrá definirse claramente en función a la información obtenida en la primera etapa, puesto que algunas auditorías pueden estar orientadas a auditar entornos muy complejos y que inclusive deben ser analizadas separadamente en función al número de entornos diferentes que cuente la Entidad, debido a que podrían responder a plataformas de hardware o tecnologías bien diferenciadas o políticas de gestión diferentes y que inclusive son manejadas en forma independiente.

Diferentes tecnologías de información pueden responder a operaciones y procesos diferentes que son administrados independientemente.

Debe quedar claramente establecido y por escrito los objetivos y delimitados los alcances de la auditoría informática. Esto nos permitirá establecer una especie de contrato entre la Entidad y la organización auditora, así mismo ayudará a estimar los costos, tiempos y plazos de ejecución de la auditoría.

3.5.3. CONFORMACIÓN DEL EQUIPO

Dependiendo del tamaño de la Entidad y la complejidad en el uso de tecnología de información, será necesario conformar el equipo de auditoría, suficiente en cantidad y calidad para llevar a cabo la auditoría informática, el seguimiento del mismo y el informe final.

En función a lo descrito, será necesario contar con el siguiente equipo de trabajo, laborando en condiciones normales:

CUADRO N° 8: CONFORMACIÓN DEL EQUIPO AUDITOR SEGÚN EL NIVEL DE COMPLEJIDAD DE LA ENTIDAD

EQUIPO / NIVEL DE COMPLEJIDAD	Gerente Auditor	Ejecutor Supervisor	Asistente	Especialista
Grande	1	2	5	*
Mediana	1	1	3	*
Pequeña	1	1	2	*

(*) En función a la complejidad de tecnología de información.

El Gerente Auditor; es el responsable de ejecutar el Proceso de Auditoría, firmará el Informe Final en representación de la Empresa Auditora.

Es el profesional con alto sentido ético que planificará, organizará y trazará estrategias para la ejecución de la auditoría; quien contando con un grupo heterogéneo logrará resultados homogéneos y sincronizados para ejecutar la auditoría y realizar el seguimiento.

El Ejecutor/Supervisor; es el responsable del trabajo de auditoría y tiene a su cargo a los asistentes sobre quienes delegará partes del trabajo, pero es la persona finalmente responsable de la ejecución de la auditoría.

Es la persona que define los requerimientos, aplica la metodología y utiliza los estándares internacionales para la detección de riesgos y controles.

Tiene a su cargo la documentación del trabajo de auditoría, la mantiene ordenada coherentemente y preparada para posibles revisiones.

Mantiene el control del tiempo asignado a cada actividad. Informa a su superior de cualquier hallazgo significativo que pueda afectar las operaciones y continuidad de la Entidad.

Discute las observaciones identificadas con las personas responsables y obtiene su comentario respectivo.

Dirige el trabajo en equipo para la determinación de las mejores prácticas de control que así lo ameriten.

Los asistentes; trabajan bajo la orientación y guía del ejecutor/supervisor y rendirán cuentas diariamente a esta persona, coordinan en equipo las recomendaciones y los efectos que podrían ocasionar los riesgos y en casos especiales o complejos el equipo determinará los mejores controles a implementar en la Entidad.

3.5.4. CRONOGRAMA DE ACTIVIDADES

El Gerente Auditor elaborará el cronograma de actividades, indicando claramente las responsabilidades y definiendo el tiempo de cada una de las actividades, para ello utilizará el Diagrama de Gantt.

Dejará previsto el tiempo necesario para la implementación de las mejoras, para su posterior seguimiento y evaluación.

Deberá también prever un tiempo prudencial para actividades imprevistas, de tal manera que le permitan cumplir satisfactoriamente con el trabajo en los plazos señalados, a fin de mantener la credibilidad de la empresa auditora.

A continuación se muestra el tiempo promedio estimado en función al tipo de Entidad o la complejidad de la misma.

CUADRO N° 9: CONFORMACIÓN DEL EQUIPO AUDITOR SEGÚN EL NIVEL DE COMPLEJIDAD DE LA ENTIDAD

PLAZO DE EJECUCIÓN / NIVEL DE COMPLEJIDAD	TIEMPO DE AUDITORÍA (días)	TIEMPO DE SEGUIMIENTO (días)	TIEMPO TOTAL (días)
Grande	90	30	120
Mediana	60	20	80
Pequeña	30	10	40

3.5.5. IDENTIFICACIÓN DE RIESGOS

Los riesgos en el uso de la tecnología y sistemas de información son evaluados en función a parámetros que fueron ampliamente explicados en la primera parte de este capítulo, los mismos que se encuentran divididos en áreas y estos a su vez en un cierto número de elementos, tal como se muestran en los cuestionarios.

Será considerado como riesgo todo aquello que impida o pone en peligro el logro de los objetivos de la organización. Por tanto en esta etapa se realizara una revisión objetiva con relación al uso de los sistemas y tecnologías de información, a fin de detectar su presencia y determinar el grado de exposición de la Entidad a la pérdida o mal uso de los servicios de los sistemas y tecnologías de información.

3.5.6. IDENTIFICACIÓN DE CONTROLES

Una vez que los riesgos han sido identificados y valorados, se puede decidir qué riesgos se deben controlar con la finalidad de orientar los esfuerzos de la organización a mitigar el efecto de la exposición de la Entidad a dichos riesgos.

Los controles que se van a realizar a través de la aplicación de la presente metodología están divididos en áreas de control y cada una de estas está sub dividida en un cierto número de elementos que han sido ampliamente explicados en la primera parte del presente capítulo.

La metodología propuesta busca en primer lugar identificar los riesgos inherentes y los factores críticos de negocio en relación con el entorno tecnológico de información, a fin de facilitar la planeación y alcance de la revisión de los controles de tecnología de información.

En esta etapa será necesario contar con especialistas en ciertas áreas de la tecnología de la información a fin de proveer las mejores prácticas para los controles de dichas tecnologías; ello va a depender del nivel de complejidad tecnológica que posea la entidad.

Los cuestionarios, muestran por otro lado el nivel de detalle de los mismos.

Es importante señalar el hecho de que se registrarán en ambos casos, tanto en la etapa de identificación de riesgos y controles, las causas que llevaron al auditor a calificar el riesgo y el control; con la finalidad de utilizar estos cuestionarios en la etapa posterior de seguimiento y para auditorías futuras, las que pueden llevarse a cabo por otros auditores, quienes deberán conocer las causas que llevaron a sus predecesores a calificar un riesgo como de alto, medio o bajo, así como a la calificación de los controles.

3.5.7. CALCULAR EL IMPACTO

Los riesgos y controles identificados deben ser valorados, considerando su nivel de impacto en función a que podrían paralizar las operaciones de la Entidad. De esta manera tendremos riesgos de alto impacto, mediano impacto y de bajo impacto.

La auditoría permite a la Entidad conocer claramente los efectos que podrían tener cada uno de los riesgos identificados y en qué medida estos podrían perjudicar su nivel de competitividad. Por tanto, la auditoría informática también entregará a la Entidad las recomendaciones necesarias para eliminar cada uno de esos riesgos o controlarlos.

3.5.8. INFORME FINAL

En esta etapa se realiza la redacción de las observaciones más importantes obtenidos durante el proceso de auditoría, indicando las causas de cada uno de ellos, los efectos, las normas que se pudieran estar infringiendo, las conclusiones y recomendaciones que debería tomar en cuenta la Entidad.

CAPÍTULO IV

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN

4.1. ANTECEDENTES

La Universidad Nacional Hermilio Valdizán de Huánuco (UNHEVAL), fue creada por Ley Nº 14915, del 21 de febrero de 1964, es persona jurídica de derecho público, con autonomía económica, normativa, académica, administrativa y de gobierno. Está integrada por profesores, estudiantes y graduados dedicados al estudio, la investigación, la difusión del saber y la cultura, y la ciencia y tecnología comprometidos con la transformación de la sociedad.

Entre los fines de la Universidad Nacional Hermilio Valdizán, Huánuco, se tiene lo siguiente:

Contribuir a la formación integral del hombre, a la transformación y desarrollo del país y al logro de una sociedad justa.

Conservar, acrecentar y transmitir la cultura universal con sentido crítico y creativo, afirmando preferentemente los valores regionales y nacionales.

Realizar investigación en las humanidades, ciencias y las tecnologías y fomentar la creación intelectual y artística, así como la cultura física.

Formar humanistas, científicos y profesionales del más alto nivel académico, de acuerdo a las necesidades de la región y del país.

Desarrollar en sus miembros los valores éticos y cívicos, las actitudes de responsabilidad y solidaridad social, el conocimiento de la realidad regional, latinoamericana y universal.

Contribuir al estudio y enjuiciamiento de la problemática regional, nacional e internacional y pronunciarse sobre ella con plena independencia de criterio planteando alternativas de solución.

Para su desarrollo las universidades consideran las siguientes funciones básicas:

a. La formación académica profesional
b. La investigación científica
c. La proyección Social
d. La Extensión Universitaria
e. La producción de bienes y servicios
f. Administración Universitaria

a. Formación Académica Profesional

Destinada a la formación profesional a nivel superior en los campos de las ciencias, la tecnología y las humanidades.

La actividad Académica de la Universidad se divide en dos grandes áreas: Pre grado y Post Grado. Las actividades de pre grado se desarrollan a través de 17 Escuelas Académico Profesionales en la Sede Central, asimismo cuenta con diversas Sedes Descentralizadas en las localidades de Margos, La Unión, Obas, Panao, Acomayo y Huácar.

b. Investigación Científica

Promueve la investigación científica, tecnológica y humanista, útil para la estructura productiva regional y del país.

La UNHEVAL cuenta con docentes investigadores en sus diferentes Escuelas Académico
Profesionales y sedes descentralizadas, los mismos que en promedio en los últimos años han realizado un promedio de 50 trabajos de investigación por año.

c. Extensión Universitaria

Las Escuelas Académico Profesionales desarrollan cursos, seminarios en sus diferentes especialidades, tales como cursos de extensión, conferencias, seminarios, fórums, coloquios, etc., dirigida a estudiantes universitarios, docentes, profesionales y público en general.

d. Proyección Social

Promueve la integración de las instituciones con participación del personal docente y estudiantes en trabajos orientados a la comunidad local y regional.

e. Producción de Bienes y Prestación de Servicios:

Propicia el funcionamiento de centro de producción de bienes y servicios, con criterio gerencial y de apoyo a la investigación científica y tecnológica.

f. Administración Universitaria

Coordina, supervisa, ejecuta y apoya acciones necesarias para el desarrollo operativo de los programas de la institución. Está orientada a brindar una estructura administrativa eficiente, ágil, flexible y automatizada, para apoyar al cumplimiento de las funciones y fines de la Universidad.

La Universidad para su funcionamiento mantiene una organización tal como se muestra en la Figura Nº 17.

De la estructura orgánica se puede observar que cuenta con los siguientes órganos de gobierno:

Órgano de Asesoramiento

Oficina de Planificación

Oficina de Asesoría Legal

Órgano de Apoyo al Rectorado

Oficina de Secretaría General

Oficina de Relaciones Públicas

Órganos de Apoyo Independientes del Vicerrectorado Académico

Dirección de Asuntos Académicos

Dirección de Servicios Académicos

Dirección de Proyección y Extensión Social

Oficina Central de Investigación

Órganos Dependientes del vicerrectorado Administrativo

Oficina General de Administración

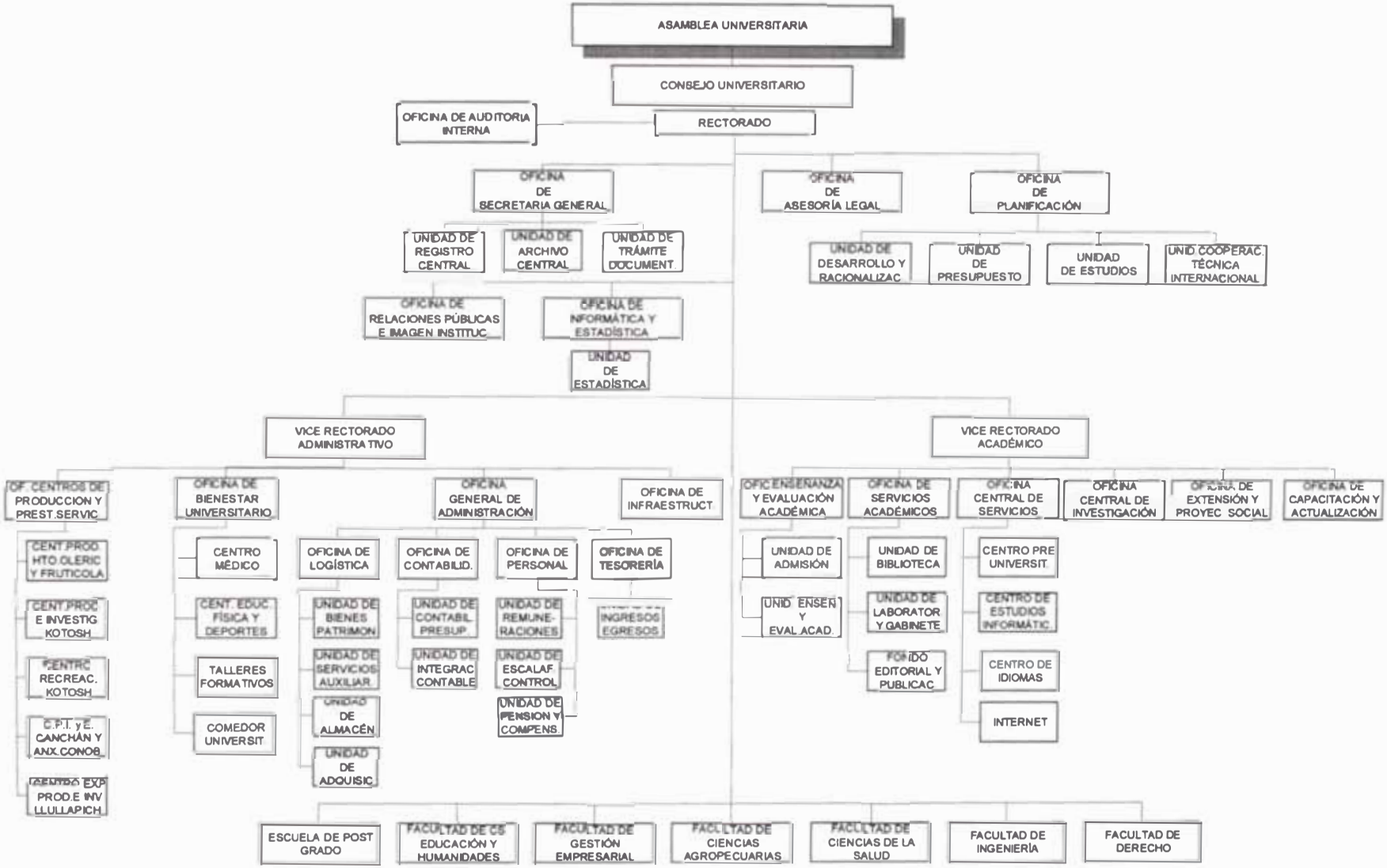
Oficina de Personal

Dirección de Bienestar Universitario

Dirección de Centros de Producción y Servicios

FIG. N° 17: ORGANIGRAMA ESTRUCTURAL DE LA UNIVERSIDAD NACIONAL "HERMILIO VALDIZÁN - HUÁNUCO

(según Resolución N° 001-AU-CR-UNHEVAL-2000



La organización socio académico-administrativa de la Universidad Nacional Hermilio Valdizán. Huánuco se sustenta en el régimen de facultades.

Las facultades son las unidades fundamentales de la organización y formación académico-profesional, integradas por profesores y estudiantes. Tienen la responsabilidad de delinear los perfiles profesionales, elaborar la currícula y coordinar los planes de estudios conducentes a la obtención de una o más especialidades donde las hubiera y certificaciones relacionadas con el ámbito de su competencia.

La Universidad cuenta con una sede central y 7 sedes descentralizadas, donde ofrece diversas carreras profesionales, para el año 2001, contaba con 6,442 alumnos matriculados, cuya demanda era atendida por 396 docentes laborando en la sede principal y 52 docentes en sedes descentralizadas. El detalle de la Información se muestra en el Anexo N° 1 y N° 2.

4.2. NORMATIVIDAD LEGAL

La Constitución Política del Perú.

La Ley Universitaria N° 23733.

Ley de creación: la Universidad Nacional "Hermilio Valdizán" de Huánuco fue creado mediante Ley N° 14915 de fecha 21 de febrero de 1964.

El Estatuto de la Universidad Nacional "Hermilio Valdizán" de Huánuco.

El Manual de Organización y Funciones fue aprobado por Resolución N° 1600-CU-CR-UNHEVAL-98.

El Reglamento de Grados y Títulos fue aprobado mediante Resolución N° 048A-PCR-UNHEVAL-98.

4.3. LEMA

"UNHEVAL, CAMINO A LA EXCELENCIA"

4.4. VISIÓN

"SER UNA INSTITUCIÓN LIDER, CONSTITUYÉNDOSE EN UNIVERSIDAD EMPRESA, PARA CONTRIBUIR AL DESARROLLO SOSTENIBLE DEL PAÍS"

4.5. MISIÓN

"SOMOS UNA INSTITUCIÓN FORMADORA DE PROFESIONALES COMPETITIVOS, GENERADORA DE CIENCIA Y TECNOLOGÍA, CON SENTIDO HUMANISTA AL SERVICIO DE LA SOCIEDAD"

4.6. PRINCIPIOS CORPORATIVOS

Las Universidades Peruanas se rigen por los principios que emana de la Ley Universitaria Nº 23733 y es como sigue:

a) La búsqueda de la verdad, la afirmación de los valores y el servicio a la comunidad.
b) El pluralismo y la libertad de pensamiento, de crítica, de expresión y de cátedra con lealtad a los principios constitucionales y a los fines de la correspondiente Universidad.
c) El rechazo de toda forma de violencia, intolerancia, discriminación y dependencia.

La UNHEVAL luego de una reunión plenaria de docentes decidió adicionar a los ya mencionados, los siguientes principios corporativos que guiarían la vida institucional a partir de ese momento.

d) CONDUCTA ETICA; Conducimos en base a los principios y valores de nuestra Sociedad
e) LIDERAZGO; Estar a la vanguardia de las organizaciones universitaria de la región
f) IDENTIDAD; Participar activamente en el desarrollo de la organización y su ámbito de influencia.
g) CONOCIMIENTO; Actualizar permanentemente al personal docente, de modo que oriente eficiente mente el aprendizaje del estudiante.
h) CREATIVIDAD; Desarrollar, innovar y adaptar ciencia y tecnología para el desarrollo de la sociedad.

4.7. OBJETIVOS ESTRATÉGICOS

Se presenta los objetivos estratégicos del macroproyecto por áreas funcionales.

MACROPROYECTO

OBJETIVOS ESTRATEGICOS	OBJETIVOS ESPECÍFICOS	METAS	ESTRATEGIAS ESPECIFICAS	UNIDADES RESPONSABLES
Realizar el proceso de Autoevalucaión Universiraria, con miras a la exelencia y calidad en el proceso de enseñanza - aprendizaje	Conformar la Comisión de Autoevaluación y Acreditación Universitaria en la UNHEVAL	Al año 2006, lograr la acreditación universitaria.	Elaboración y aprobación del Reglamento para la Autevaluación.	Rectorado - Vicerrectorados
			Elaboración y aprobación del Reglamento para la Acreditación Universitaria.	Rectorado - Vicerrectorados

A. AREA ACADÉMICA

OBJETIVOS ESTRATEGICOS	OBJETIVOS ESPECÍFICOS
Formar profesionales y post graduados de alto nivel científico, humanístico y empresarial para atender las necesidades de la región del país.	Implantar estructuras curriculares que respondan a las exigencias profesionales del área de influencia de la UNHEVAL, teniendo en cuenta las exigencias del mercado laboral futuro.
	Establecer programas académicos permanentes como refuerzo y complemento de la información profesional.
	Implantar modernos sistemas de aprendizaje apoyados con tecnología de última generación y material didáctico adecuado para tal fin.
	Plana docente altamente competitiva.
	Establecer servicios de bibliografía y otros a través de la biblioteca central, equipada con tecnología de última generación y de las bibliotecas especializadas de las EAP.
	Crear nuevas carreras en función de las necesidades de la región y según los avances de la ciencia y tecnología.
	Mantener el sistema de titulación profesional vía tesis y la titulación especial. Promover el ingresos de alumnos y egresados en el mercado laboral.
	Potenciar a la escuela de post grado con la asignación y generación de recursos económicos y la consolidación de una plana docente de alto nivel académico.

B. AREA: INVESTIGACION

OBJETIVOS ESTRATEGICOS	OBJETIVOS ESPECÍFICOS
Crear nuevos conocimientos tecnicos y procedimientos de investigación, acorde a las necesidades y potencialidades de la región y el país.	Potenciar, reestructurar e implementar la Oficina Central de Investigación.
	Repotenciar e incentivar la actividad investigativa de docentes, alumnos y egresados de la UNHEVAL.
	Difundir oportunamente los conocimientos científicos, tecnológicos y humanísticos generados en la UNHEVAL.

C. AREA: PROYECCION SOCIAL Y EXTENSION UNIVERSITARIA

OBJETIVOS ESTRATEGICOS	OBJETIVOS ESPECÍFICOS
Desarrollar programas de proyección social hacia la colectividad, en búsqueda del desarrollo de los sectores sociales, ofreciendo alternativas de solución a sus necesidades, mediante la transferencia de conocimientos científicos tecnológicos.	Lograr la presencia permanente y preponderante de la UNHEVAL en el espacio regional y nacional, posibilitando una mayor promoción del desarrollo.
	Difundir oportunamente los conocimientos científicos, tecnológicos y humanísticos generados en la UNHEVAL.
	Promover la generación y transmisión de conocimientos científicos, tecnológico y cultural con el fin de apoyar a la población a mejorar su calidad de vida.
	Lograr la presencia de la UNHEVAL en las instituciones líderes de la región y el país.

D. AREA: BIENESTAR UNIVERSITARIO

OBJETIVOS ESTRATEGICOS	OBJETIVOS ESPECÍFICOS
Ofrecer servicios complementarios de calidad a favor de los estamentos de la universidad.	Asignar adecuadamente las áreas de estudio a los estudiantes.
	Implementar un programa de servicio asistencial básico
	Promover la práctica de actividades artísticas y culturales.
	Vincular las acciones de extensión universitaria con instituciones educativas.-

E. GESTION ACADEMICA ADMINISTRATIVA

OBJETIVOS ESTRATEGICOS	OBJETIVOS ESPECÍFICOS
Lograr una gestión académica y administrativa eficiente y competitiva, que permita la asignación óptima y uso racional de los recursos para el cumplimiento de los objetivos institucionales.	Reformular y reglamentar las normas que rigen la vida académica y administrativa de la UNHEVAL permitiendo implantar procesos y servicios académicos administrativos.
	Implantar procesos y servicios academicos-administrativos, que apoyados con tecnología de punta y medios adecuados, permitan una gestión óptima.
	Lograr que el personal docente y administrativo tengan un alto grado de calificación profesional y técnica que dirija y ejecute eficientemente los procesos académico administrativos.
	Establecer un sistema de planificación participativa - acción, que promueva la gestión y asignación de los recursos de las distintas unidades académicas y administrativas.
	Consolidar la infraestructura de la ciudad universitaria.
	Celebrar convenios y acuerdos específicos con Universidades e Instituciones del país y el extranjero para programas de intercambio Técnico científico, convenios para programas de capacitación y prestación de servicios.
	Establecer permanentes vínculos con instituciones públicas y privadas regionales y nacionales, para fortalecer la imagen y el liderazgo institucional.
	Implementar sistemas de auditoría, para un eficaz control y evaluación de la gestión académica, administrativa y financiera de la UNHEVAL Repotenciar los Centros de Producción y de Servicios con el objeto de incrementar la capacitación de recursos propios.
	Impulsar la organización y funcionamiento de nuevos centros de producción y de servicios para incrementar la captación de recursos propios.

4.8. PROCESOS DE NEGOCIO

De la Cadena de Valor mostrada en la Figura Nº 18 se pueden identificar las funciones claves que desarrolla la Universidad para su normal funcionamiento. Una vez determinadas las funciones es necesario identificar a partir de ellas, los procesos más importantes que desarrolla y que son susceptibles de automatización.

Por tanto, para descubrir los procesos más importantes de la Universidad, la dividiremos en sus dos Areas Básicas, las mismas que corresponde exactamente a las actividades primarias y apoyo mostradas en la cadena de valor actual de la UNHEVAL.

Area Administrativa

Area Académica

4.8.1. ÁREA ADMINISTRATIVA

PROCESO DE FORMULACIÓN Y EVALUACIÓN DEL PRESUPUESTO DE LA INSTITUCIÓN

Este proceso se inicia con la recopilación de Requerimientos Anuales de todas las Unidades Académicas, Administrativas y de Producción de la Universidad, las que se cuantifican, valorizan y se encuadran en base al Marco Presupuestal otorgado por el Gobierno Peruano y la proyección de los Ingresos Propios generados por la Universidad.

Por tanto se genera los siguientes procedimientos:

Formulación del Presupuesto de la Universidad según Partidas presupuestarias y origen del fondo de funcionamiento(ingresos propios, estado, donaciones, etc).

Programación del Presupuesto Trimestral y Mensual.

Seguimiento y Control de los Calendarios de Compromiso.

Ejecución del Gasto y los Ingresos.

Evaluación de la Ejecución Presupuestal.

Obtención de Reportes Estadísticos.

Obtención de Reportes de Resumen

FIG. N° 18. CADENA DE VALOR ACTUAL – U N H E V AL

GESTIÓN UNIVERSITARIA:	Planificación Universitaria Gestión académica Relaciones Gubernamentales	Convenios nacionales e internacionales Gestión contables y financiera Gestión de la Tecnología y Sistemas de Información
INVESTIGACIÓN Y DESARROLLO	Capacitación Financiamiento a la investigación	Publicación de la investigación Transferencia Tecnológica
ADMINISTRACIÓN DE PERSONAL:	Selección promoción y evaluación de personal Reconocimientos e incentivos	Control de asistencia Desarrollo administrativo
ABASTECIMIENTO:	Compra de materiales, suministro, servicios Compra de materiales didácticos, activos	Control de activos Mantenimiento de infraestructura

LOGÍSTICA INTERNA	**OPERACIÓN**	**LOGÍSTICA EXTERNA**	**MARKETING**	**VENTAS**	**SERVICIO POST VENTA**
LOGÍSTICA DE LA INFORMACIÓN Compra de material bibliográfico Obtención de información por INTERNET Obtención de Videos de capacitación **LOGÍSTICA DE LA ENSEÑANZA** Interacción metodológica Programación de la clase Entrega de separatas	**PROCESO ENSEÑANZA APRENDIZAJE** vestigación bibliográfica Estudio de Casos reparación de syllabus Preparación de clase	**INCREMENTO DE CONOCMIENTO**	**MARKETING** Publicidad Identificación de clientes Imagen de las unidades estratégicas	**VENTAS** Transmisión del conocimiento	**SERVICIO POST ENSEÑANZA** *Atención a los graduandos* *Consejería y Asesoría a los estudiantes*

La Unidad responsable de ejecutar este proceso es la Dirección de Planificación y para su ejecución debe coordinar las unidades de Logística, Contabilidad, Remuneraciones, Tesorería, Alta Dirección, Facultades, Centros de Producción.

PROCESO DE ABASTECIMIENTO DE BIENES Y SERVICIOS

Tiene como función proveer de bienes, materiales y servicios a todas las unidades orgánicas de la Universidad para garantizar su normal funcionamiento. Para cumplir con sus funciones realiza los siguientes procesos de importancia:

Adquisición de bienes y servicios.

El objetivo fundamental de este sub-proceso es adquirir los bienes y servicios de acuerdo con la normatividad vigente, proveyendo de bienes y servicios de calidad, en el tiempo oportuno y al precio más económico.

Inventario de Bienes Patrimoniales de la Institución.

Tiene por objeto mantener actualizado y valorado el inventario de bienes muebles e inmuebles de la institución, para su control, preservación y comunicación a la Superintendencia Nacional de Bienes del Estado.

Almacenamiento de Bienes

Controla el ingreso y salida de bienes de almacén. Mantiene actualizado el stock de bienes. Valoriza los bienes que salen de almacén.

Para la ejecución de sus funciones coordina con las oficinas de Planificación, Contabilidad, Tesorería, Facultades y Unidades de Producción.

PROCESO CONTABLE

Tiene a su cargo la elaboración y evaluación de los estados financieros contables y bancarios.

Para cumplir con este proceso realiza los siguientes sub-procesos de importancia:

Elaboración del Balance de Comprobación.

Formular los Estados Financieros.

Realizar la integración contable de los bienes, fondos, presupuesto y pensiones o compensaciones.

Realizar Conciliaciones Mensuales del presupuesto con la ejecución del gasto.

Controlar la Ejecución Presupuestal a nivel de programas, fuente de financiamiento, partidas proyectos y obras.

Coordina con las áreas de logística, Remuneraciones, Tesorería y Planificación.

PROCESO DE CONTROL Y EVALUACIÓN DE INGRESOS Y EGRESOS

A cargo del área de Tesorería, cuyo objetivo es controlar y cautelar los recursos directamente recaudados, así como los egresos de las diferentes cuentas de recursos ordinarios de acuerdo con las autorizaciones de giro.

Los procesos que realizan para cumplir con los objetivos son:

Registrar y controlar la captación de ingresos propios de la Institución.

Registrar y controlar la ejecución del movimiento de fondos de recursos ordinarios y los directamente recaudados.

Realizar Conciliaciones bancarias.

Mantener la Cuenta Corriente de cada alumno.

4.8.2. ÁREA ACADÉMICA

El área académica es uno de los pilares de toda institución universitaria, por lo tanto constituye un factor clave de éxito su planeamiento, desarrollo y evaluación.

El objetivo fundamental es la formación profesional del estudiante, para ello debe garantizar una correcta selección de estudiantes, garantizar una plan docente, brindar el uso de laboratorios y aulas para la enseñanza.

Los procesos más importantes en el área académica son:

PROCESO DE ADMISIÓN

Este proceso se inicia con la inscripción de postulantes al Examen de Admisión por Concurso de Selección, por las siguientes modalidades: Selección General, Traslado Interno y Externo, Primeros Puesto de Colegio, Segunda Profesión.

La Universidad cuenta con un Centro Pre Universitario que otorga vacantes para el ingresos directo a la Universidad a sus primeros puestos. Estos estudiantes se someten a tres procesos de evaluación por ciclo.

A continuación se realiza la evaluación del postulante a través de la administración de una prueba, la que es calificada para luego publicar y distribuir sus resultados.

PROCESO DE MATRÍCULA

El proceso de matrícula, tiene por objeto registrar adecuadamente a los alumnos como estudiantes de la Universidad, garantizar su inscripción en las asignaturas correspondientes y controlar los pagos por derecho de matrícula y ensenanza.

La Universidad mantiene dos sistemas de régimen de estudios: El Sistema Anual y el Semestral. Por lo tanto existen un proceso de matrícula por año y pueden existir dos procesos de inscripción por cursos.

La tasa de pago de Matrícula está en función al número de cursos desaprobados en el año de estudios anterior.

La inscripción por asignaturas debe controlar la aprobación previa de cursos pre-requisitos y el año de estudios en que se encuentra el alumno.

Los pagos por derechos de enseñanza mensual corresponde a los alumnos que tienen más de dos cursos desaprobados en el año académico anterior.

Los Reportes más importantes que genera este sistema son:

Récord Académico del Alumno.

Récord de Pagos del Alumno.

Listas de Inscripción de Alumnos por Asignaturas

Listas de Inscripción de Alumnos por Año de Estudios

Actas de Notas

Registros de Asistencia

Registros de Evaluación

Además se genera Indicadores de Rendimiento Académico por alumno, Escuela, etc.

PROCESO DE CONVALIDACIÓN DE ASIGNATURAS

Este proceso es particularmente importante porque la Universidad esta pasando progresivamente del régimen anual al semestral en sus 23 Escuelas Académico Profesionales y consiste en adecuar a un alumno de una currícula de estudios a otra vigente, otorgándose convalidaciones de una signatura a otra.

4.9. INFRAESTRUCTURA DE TECNOLOGÍA DE INFORMACIÓN DE LA UNIVERSIDAD

La Universidad Nacional Hermilio Valdizán, administra básicamente tres redes LAN:

1. Red Internet:

   Destinada a al uso intensivo de acceso a INTERNET, a disposición de los alumnos, docentes y administrativos a un precio módico de S/. 100 la hora.
   La red se encuentra instalada bajo topología estrella y es administrada por un Ing. Electrónico.
   Atiende 12 horas diarias de 8.00 a.m. a 8.00 p.m. en forma ininterrumpida.
   Cuenta con el siguiente equipamiento:
   Línea dedicada alquilada de Telefónica, con un ancho de banda de 512 Kbps.
   Un Router
   Un modem
   Un Switcher
   Cuatro Hubs Ethernet
   65 Computadoras: Celeron 450 Mhz, 4.2 GB de Disco Duro, 128 Mb de memoria RAM, Disketera de 3.5"
   Sowtare base: Windows 98.
   Otros software: Internet explorer, office 98, antivirus Hacker.

2. Red Administrativa:

   Destinada a dar soporte al área administrativa, actualmente únicamente da soporte a la Oficina de Contabilidad y Tesorería; mientras que las oficinas de Planificación, Logística y Remuneraciones trabajan en Computadoras Stand Alone.

Es una red de topología estrella basada en ETHERNET 10 Base T, el protocolo que usa es el NETBEUI.

Cuenta con el siguiente equipamiento:

Un servidor Pentium III de 450 MHZ, 128 Mb de memoria RAM, 10.2 Gb de Disco Duro, MODEM Interno de 64 Kbps. Lectora de CDs.

1 HUB de 16 puertos

5 Computadoras entre Pentium I,

1 computadora Pentium IV

1 computadora Pentium III

1 computadoras Pentium II

5 impresoras de inyección a tinta

3 impresoras matriciales FX 1170

Software Base: Windows NT para el servidor y para los usuarios Windows 98

Software Aplicado: SIAF, Sistema de Ingresos.

Otros Software: Office 98.

3. Red Académica

Sirve para dar soporte al área académica de la Universidad. La información académica se encuentra centralizada en la Oficina de Informática y estadística y la red se encuentra instalada únicamente en ésta dependencia.

Es una red de topología estrella 100 Base T que tiene el siguiente equpamiento:

1 Servidor Pentium III 450 Mhz, 128 Mb de RAM, disco duro de 10 GB

Número de terminales: 4 Pentium I y II

Plataforma: Novell 4.1

Dos lectores ópticos: Para calificación de exámenes de Centro Pre Universitario, Admisión, evaluaciones diversas de alumnos y lectura de Actas de Notas.

Cámara Digital: Para la obtención de la imagen del alumno.

1 Impresora Laser

1 Impresora Matricial.

Lectora grabadora de CD

Zipeador

Regrabadora de CD

Sobre ésta red corre únicamente el sistema académico de la universidad, desarrollado en fox pro para DOS.

La red también está conectada a INTERNET.

Las demás oficinas administrativas, académicas y los centros de producción de la Universidad, están equipadas con computadoras individuales y con software base: Windows 98 y el paquete Office 97.

Area de Gestión Académica:

Conformada por las Facultades, Institutos de Investigación, Escuela de Post Grado, Centro Pre Universitario, Biblioteca, Admisión. Estas oficinas se encuentran implementados parcialmente con las siguientes computadoras para realizar tareas de gestión.

Computadora 486 DX	10
Computadora Pentium I	25
Computadora Pentium II	28
Computadora Pentium III	34
Total	97

Area Administrativa:

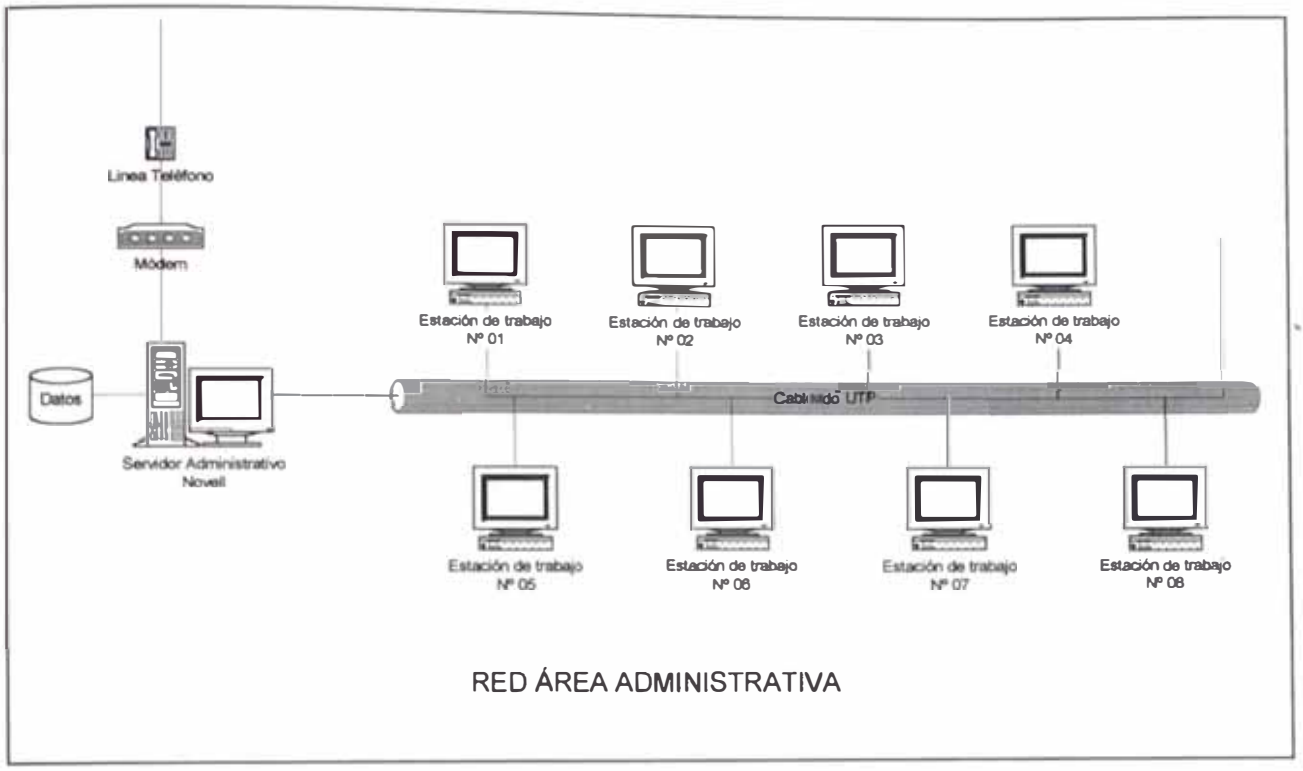
Conformada por aquellas oficinas administrativas, que no se encuentran interconectadas a las redes LAN de la universidad.

Computadora 486 DX	16
Computadora Pentium I	34
Computadora Pentium II	42
Computadora Pentium III	37
Total	129

Centros de Producción:

Conformado por el Centro de Idiomas, Centro de Estudios Informáticos, Centro de Producción Llullapichis.

Computadora 586	36
Computadora Pentium I	4
Computadora Pentium II	24
Total	64



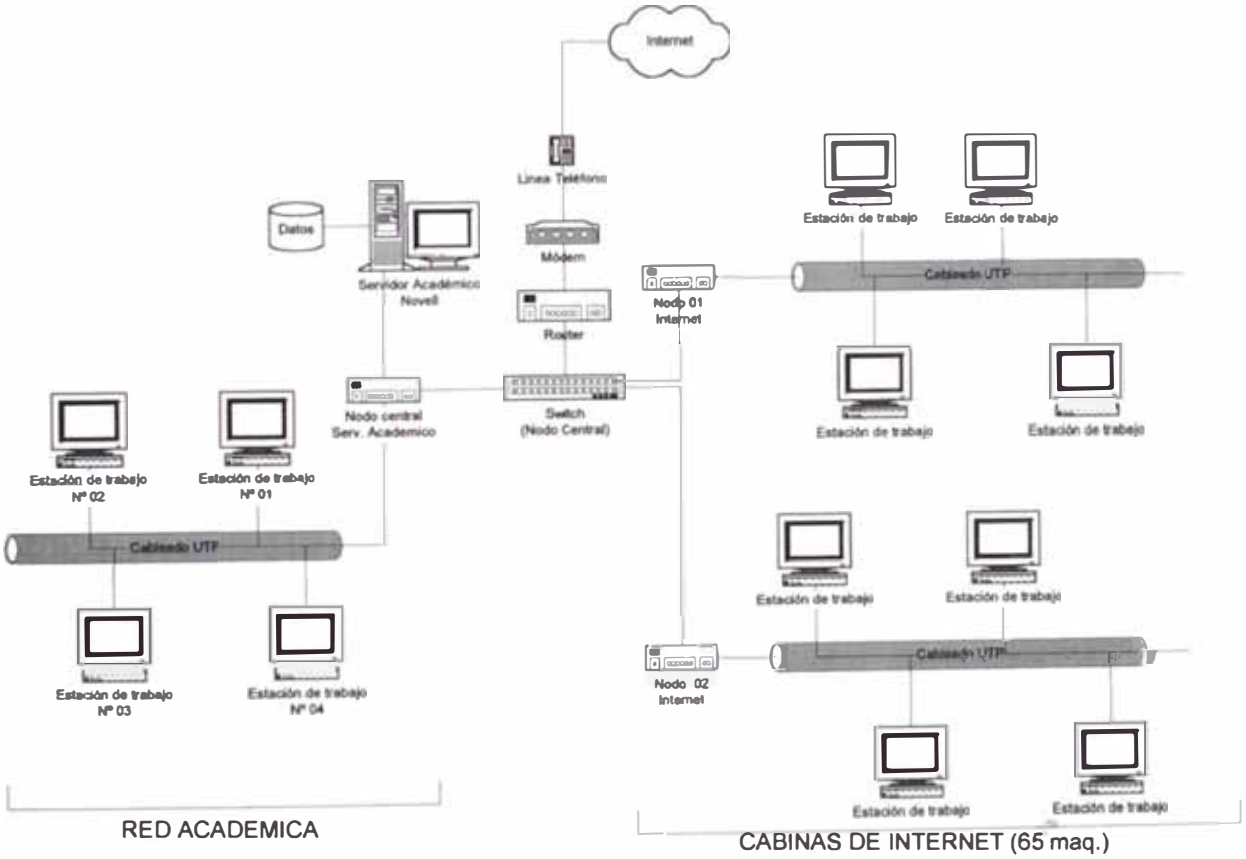


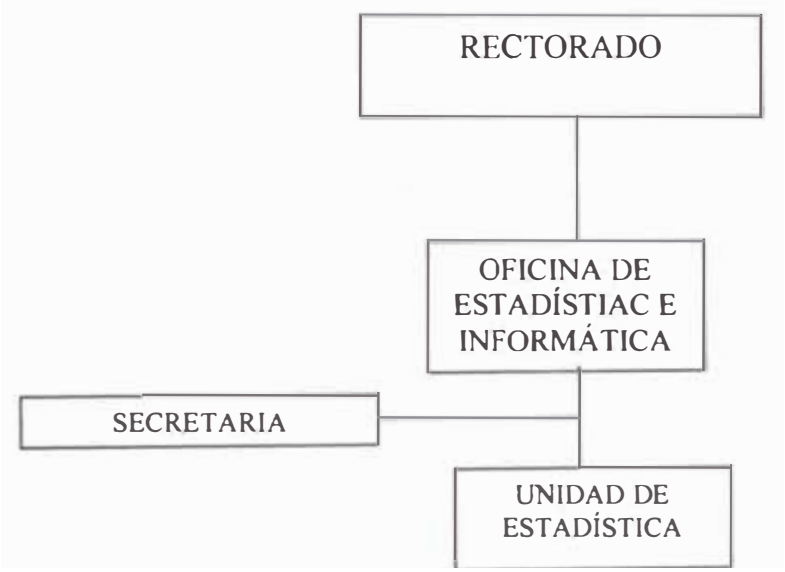
FIG. N° 19 Diseño arquitectónico de redes de la UNHEVAL

4.10. DESCRIPCIÓN DEL ÁREA DE INFORMÁTICA DE LA UNIVERSIDAD

La Oficina de Estadística e Informática de la Universidad Hermilio Valdizán es una unidad dependiente de la Dirección de Asuntos Académicos.

La estructura orgánica es la siguiente:

FIGURA N° 20: ESTRUCTURA ORGÁNICA DEL ÁREA DE INFORMÁTICA Y ESTADÍSTICA DE LA UNIVERSIDAD NACINAL HERMILIO VALDIZÁN



Las funciones asignadas al oficina de estadística e informática y los cargos administrativos designados son los siguientes:

FUNCIONES ESPECIFICAS:

Las funciones generales que aquí se describen son las que se encuentran en el manual de Organización y Funciones de la Universidad.

- Planificar, organizar, dirigir, ejecutar y controlar los procesos técnicos y operacionales de computo e informática.

  Producir y difundir cómputos e informes confiables y oportunas que permiten conocer variables de la realidad universitaria.

  Proponer proyectos de convenios con instituciones nacionales e internacionales para la implementación de la Red Informática e Internet.

  Brindar apoyo y coordinar permanentemente con los órganos de la institución, para establecer nuevos diseños informáticos a fin de optimizar sus funciones.

  Proponer políticas de mantenimiento y seguridad de las computadoras de la UNHEVAL en su conjunto.

  Mantener actualizado el Registro Académico de la Universidad.

  Centralizar, procesar, consolidar y evaluar la información estadística institucional, a fin de ser utilizada como instrumento de gestión técnico administrativo en la toma de decisiones.

Los trabajadores de esta oficina son los siguientes:

JEFE DE OFICINA DE ESTADÍSTICA E INFORMÁTICA

Economista Nicéforo Peña Valdivia

ANALISTA DE SISTEMAS PAD

Ing. Industrial Manuel Domínguez Cuellar

OPREADORES PAD

Bachiller en Economía: Javier Ochoa Padilla

Bachiller en Contabilidad: Freddy Noreña Tello

SECRETARIA

Señorita Sara Garay Arteta

Los procesos de negocio que se encuentran directamente a su cargo son los de matrícula y admisión.

4.11. DIAGNÓSTICO DE LA UNIVERSIDAD

Para el diagnóstico de la Universidad se tomó en cuenta primeramente el análisis interno y el externo, los mismos que se detallan a continuación.

4.11.1. ANÁLISIS INTERNO

Para ello se realizó un proceso de Auditoria Interna y se identificó las fortalezas y debilidades a nivel de la institución, en base a las siguientes capacidades:

Capacidad Organizacional

En esta etapa se analizó todas aquellas fortalezas y debilidades que tengan que ver con el proceso administrativo en planeación, dirección, toma de decisiones, comunicaciones y control.

Capacidad, calidad y evaluación de gestión

Comunicación y vínculo institucional

Ambiente Organizacional

Reglamentos internos

Sistema de toma de decisiones

Plan de Desarrollo Estratégico

Descentralización de Escuelas

Plan Curricular

Consejería y asesoría

Convenio con otras instituciones

Servicios académicos, entre otros.

Capacidad de Talento Humano

En donde se incluye: Nivel académico, experiencia técnica, nivel de remuneración, capacitación, motivación, identidad institucional, etc.

- Creatividad e innovación (talento humano)
- Estabilidad laboral
- Motivación
- Especialización de personal
- Calidad de docentes
- Actitud de cambio e innovación de docentes
- Nivel de desempeño y gestión, entre otros.

Capacidad de Infraestructura

- Pabellones de aulas
- Pabellón de atención administrativa.
- Laboratorios
- Biblioteca
- Complejo deportivo
- Áreas verdes
- Servicios higiénicos, entre otros.

Capacidad Tecnológica

Incluye entre otros: infraestructura tecnológica (hardware), nivel tecnológico, disponibilidad de software, procedimientos administrativos, procedimientos técnicos y laboratorios.

- Uso de medios audiovisuales
- Centro Informático e Internet
- Capacidad de innovación
- Maquinaria básica de producción
- Nivel de automatización, entre otros.

Capacidad Financiera y Presupuestal

Incluye todos los aspectos relacionados con las fortalezas y debilidades financieras de la universidad, tales como: disponibilidad de líneas de crédito, capacidad de endeudamiento, generación de recursos propios, asignación presupuestal del Tesoro Público.

Capacidad Competitiva

Todos los aspectos relacionados con el área comercial, tales como calidad del servicio educativo, exclusividad, participación de mercado, desarrollo y proyección social, gestión empresarial.

- Imagen y liderazgo institucional
- Escuela de Post Grado
- Centro de Idiomas
- Rendimiento Académico
- Calidad de Investigación Científica y Tecnológica

- Centros de Producción, entre otros.

Las capacidades se evaluaron en base a los criterios señalados líneas arriba, los mismos que se calificaron como una fortaleza o una debilidad de la UNHEVAL, así mismo se determinó el impacto que representa para hacer frente al medio competitivo. Los resultados de esta medición se muestran en el Anexo N° 3.

Según el documento oficial instructivo N° 001-2000-EF/76.01, se considera los siguientes ítem relacionados con la UNHEVAL:

A) Usuarios

- Estudiantes egresados del nivel secundario
- Estudiantes de institutos superiores
- Profesionales
- Bachilleres
- Oficiales de las Fuerzas Armadas.
- Comunidad
- Instituciones Naturales
- Instituciones Jurídicas
- Instituciones Públicas
- Instituciones Privadas

B) Beneficiarios

- Sociedad
- Instituciones Naturales
- Instituciones Jurídicas
- Instituciones Públicas
- Instituciones Privadas

C) Proveedores

- Empresas editoras
- Universidades públicas y privadas
- Centros Educativos privados y públicos
- Centros de investigación
- Empresas de servicio público
- Empresas de distribuidoras de materiales de oficina
- Empresas de venta de maquinarias y equipos

D) Entidades que prestan Servicios Similares

- Universidad Privada Huánuco
- Institutos Superiores Tecnológicos y Pedagógicos
- Universidad Nacional Agraria de la Selva
- Universidad Nacional Daniel Alcides Carrión de Cerro de Pasco
- Universidad Nacional del Centro del Perú – Huancayo
- Universidad Particular de los Andes - Huancayo

E) Otras Entidades Estatales que se relacionan con la Universidad

- Comité Transitorio de Administración Regional – CTAR Huanuco.
- Colegios Profesionales
- Iglesias
- Ministerio de Agricultura
- Ministerio de Salud
- Ministerio de Educación
- INEI
- PROFINES
- Dirección Regional de Industria Turismo y Comercio
- EsSalud, Hospital Hermilio Valdizán
- Institutos Educativos
- Entidades No Estatales que se relacionan con la Universidad
- ONG's
- Entidades Cooperantes Internacionales: Cuba, Chile, Holanda.

4.11.2. ANÁLISIS EXTERNO

Para realizar el análisis externo, es necesario conocer en primer lugar en qué tipo de sector se desenvuelve la Entidad, determinar con quienes compite y se relaciona, para ello utilizamos las Cinco Fuerzas Competitivas de Porter, que se muestra en la Figura Nº 21.

Para calcular el impacto de las amenazas y oportunidades se han analizado los siguientes factores, en base a los cuales se ha preparado el Perfil de Oportunidades y Amenazas del Medio, mostrado en el Anexo Nº 4.

Factores Económicos

Relacionados con el comportamiento de la economía, el flujo de dinero, bienes y servicios, tanto a nivel nacional e internacional, considerando su incidencia para nuestra organización. Los factores más relevantes fueron:

- Recesión económica
- Inflación
- Acceso a las fuentes de financiamiento externo y/o donaciones
- Ley de Presupuesto Público
- Privatización
- Apoyo del Gobierno a las instituciones públicas
- Existencia de instituciones financieras
- Globalización económica
- Crecimiento económico, entre otros.

Factores Geográficos

Se registró los de mayor incidencia entre los que encontramos:

- Clima
- Diversidad de flora y fauna
- Ubicación
- Área de influencia
- Expansión urbana
- Fenómenos adversos de la naturaleza, entre otros.

Factores Demográficos

Los indicadores poblacionales más importantes son:

- Migración
- Tasa de mortalidad
- Crecimiento poblacional

Factores Políticos

Los que están referidos al uso o asignación del poder, en relación con los gobiernos nacionales, regionales, locales, etc.

- Ley de Promoción de la Inversión en la Amazonía
- Integración multisectorial

- Estabilidad Política
- Creación de entidades de desarrollo
- Nuevas tendencias en la educación, entre otros.

Factores Legales

- Ley Universitaria N° 23733
- Ley del Servidor Público - 276
- Ley de Promoción a la Inversión en la Amazonía
- Estatuto
- Reglamentos
- Resolución de Fusión de facultades

Factores Sociales

Los que afectan el modo de vivir de la gente, incluso sus valores (educación, salud, empleo, seguridad, etc.) relacionadas con la política social del país.

- Pobreza y Pobreza Extrema
- Desempleo y subempleo
- Fuga de talentos
- Participación ciudadana en el desarrollo local
- Crisis de valores, delincuencia
- Pacificación Nacional, entre otros.

Factores Culturales

Respecto a nuestros valores culturales consideramos los siguientes:

- Falta de identidad
- Manifestaciones artísticas, musicales, deportivas y literarias
- Legado histórico, entre otros.

Factores Tecnológicos

Los relacionados con el desarrollo de las máquinas, las herramientas, los procesos, los materiales, etc. Son:

- Globalización tecnológica
- Tecnología de manejo organizacional
- Industrias Agropecuarias Regionales
- Desarrollo de la tecnología informática
- Transferencia tecnológica, entre otros.

Resultado del análisis de cada uno de los factores, estos se han clasificado en fortalezas y debilidades para la institución, mediante la matriz POAM, que se muestra en el Anexo Nº 4.

Con ambas matrices, POAM y PCI, se ha elaborado la matriz FODA, conocida como Matriz de Fortalezas, Oportunidades, Debilidades y Amenazas, con la finalidad de definir las estrategias de la institución.

Es oportuno mencionar que la autora del presente trabajo de investigación participó en la elaboración del Plan de Desarrollo de la Institución 2001-2006, aprobado con Resolución de Consejo de Facultad, en calidad de Directora de la Escuela Académico Profesional de Ingeniería Industrial, durante el año 2001.

La Matriz FODA se presenta en el Cuadro Nº10, donde se pueden apreciar las estrategias ofensivas, defensivas, adaptativas y de supervivencia. Se observa que el componente tecnológico se encuentra presente por lo menos a nivel de Planeamiento Estratégico, demostrando que existe conciencia de la necesidad de hacer uso de las tecnologías de la información.

CAPÍTULO V

AUDITORÍA INFORMÁTICA

Una vez completada la primera fase de la realización del proceso de Auditoría Informática en la Universidad Nacional Hermilio Valdizán, se tendrá un profundo conocimiento de la entidad y en función a ello se podrán determinar los objetivos y alcance de la Auditoría Informática a realizar; de la misma manera se podrá designar el personal suficiente y capaz para llevar a cabo esta tarea, cronogramar sus actividades con fines de supervisión y cumplimiento de planes establecidos.

5.1. OBJETIVOS DE LA AUDITORÍA INFORMÁTICA

Para la definición de objetivos se coordinó con la Alta Dirección de la Universidad, con la finalidad de llegara un acuerdo respecto a los fines de la presente Auditoría Informática, los mismos que debían estar en concordancia con el presente trabajo de investigación:

- Identificar riesgos en el uso de tecnología de la información
- Evaluar controles en el uso de tecnología de la información
- Evaluar el impacto de los riesgos en el uso de tecnología de la información
- Definir plazo de ejecución de las mejoras

5.2. ALCANCE DE LA AUDITORÍA INFORMÁTICA

El proceso de Auditoría Informática a aplicarse en la Universidad Nacional Hermilio Valdizán de Huánuco, abarca a la Oficina de Informática de la Entidad y su relación con las áreas académica y administrativa.

5.3. EQUIPO DE TRABAJO DE AUDITORÍA DE SISTEMAS

La Universidad está considerada como una Entidad de tamaño y complejidad de grado medio; debido a que cuenta con aproximadamente 400 docentes que laboran en el área académica, 300 trabajadores del área administrativa y 6,500 alumnos. Por otro lado cuenta con 3 redes LANs y tienen a su cargo el mantenimiento de 290 computadoras de diversa tecnología y otros equipos informáticos.

Por tanto se ha trabajado con el siguiente equipo de trabajo:

Ejecutor y/o Supervisor		Ing. Guadalupe Ramírez Reyes
Personal Asistente	:	Ing. Víctor Campos Medina
		Ing. Manuel Domínguez Cuellar

Las funciones del Gerente Auditor, fueron cumplidas por la tesista, estando a mi cargo la planificación, conformación del equipo, la realización de las iversas gestiones que permitieron aplicar la Auditoría Informática en la Universidad Hermilio Valdizán y por último responsable de la Auditoría.

Durante el desempeño de las funciones de Ejecutor/Supervisor, se han realizado las siguientes actividades:

- Preparar la carta de requerimiento, incluyendo la información necesaria requerida para el trabajo.
- Elaborar la estrategia y la planificación de la auditoría
- Aplicar la metodología propuesta y estándares de auditoría y control de aceptación internacional.
- Obtener la información más importante de los principales procesos y actividades
- Documentar los hallazgos obtenidos en el trabajo de campo
- Mantener una documentación ordenada y coherente
- Mantener un control del tiempo asignado a las actividades

- Discutir las observaciones identificadas con las personas responsables y obtener su comentario respectivo
- Preparar el informe de la auditoría efectuada.

El personal asistente, trabajó en coordinación estrecha con el ejecutor de la auditoria. Después de cada día de trabajo en la Entidad el equipo de trabajo realizaba reuniones de evaluación, coordinación, discusión de los mejores controles, determinación de los impactos debido a riesgos presentes, con la finalidad de emitir un informe altamente confiable.

5.4. CRONOGRAMA DE EJECUCIÓN

De acuerdo a la complejidad de la Entidad determinada en el punto anterior y habiendo definido el equipo que participará en el proceso de Auditoría se ha realizado el siguiente cronograma de trabajo, mostrado en el Cuadro Nº 11.

El tiempo total calculado fueron de 2 meses para la ejecución del proceso de auditoría, sin considerar los trámites realizados en la Entidad sujeto de nuestra investigación.

5.5. APLICACIÓN DE CUESTIONARIOS

A continuación presentamos los diferentes cuestionarios que fueron aplicados durante el proceso de Auditoría Informática. Se muestra en cada uno de ellos los comentarios respecto a los puntos evaluados, resultado de la auditoría.

CUADRO Nº : 11

CRONOGRAMA DE ACTIVIDADES DEL PROCESO DE AUDITORÍA INFORMÁTICA

ACTIVIDAD	TIEMPO							
	DICIEMBRE 2001				ENERO 2002			
	SEM 1	SEM 2	SEM 3	SEM 4	SEM 5	SEM 6	SEM 7	SEM 8
1. Coordinación con la Entidad (*)								
2. Entendimiento de la Entidad								
2.1. Entendimiento organizacional								
2.2. Descripción de los Procesos de Negocio								
2.3. Infraestructura Tecnológica								
2.4. Descripción del Área de Informática								
2.5. Diagnóstico de la Organización								
3. Determinación de los Alcances y Objetivos								
4. Identificación de Riesgos								
5. Identificación de Controles								
6. Elaboración del Informe Final								
7. Imprevistos (**)								

(*) 15 días de trámite con la Entidad

(**) 1 semana adicional

FUENTE: Elaboración Propia.

RIESGOS DEL AREA DE INFORMÁTICA

Cuadro N° 1	**Hoja N° _1___ de _____**
Entidad: Universidad Nac.Hermilio Valdizán	**Año Auditado: Diciembre / 2001**
Auditor encargado: Ing. Guadalupe Ramírez	**Fecha: Enero / 2002**
Auditor revisor: _____	**Fecha: _____/_____**

Evalúe lo siguiente	Exponga sus comentarios
Anote las implicancias para la auditoria de los siguientes riesgos y su relación con objetivos específicos de auditoria y la participación de especialistas. Factores de riesgos de TI a evaluar: **• Dependencia en TI** Evalúe: - El nivel de mecanización de los procesos de negocio de la Entidad. - La sofisticación con respecto a la entrega de información en tiempo real y que influye en la toma de decisiones. - La información que se genera en las áreas usuarias y la protección establecida considerando las normatividad vigente. - El tiempo que podría esperar la Entidad sin dar atención a los usuarios o clientes, a organismos reguladores; debido a la inoperatividad de su infraestructura tecnológica.	Los sistemas académicos y administrativos tienen mayor impacto en el negocio de la Universidad y fallan. Se tiene una dependencia moderada en los recursos de la Oficina de Informática La Entidad podría paralizar sus actividades académicas en un plazo no mayor a 10 días; mientras que las actividades administrativas solo podrían soportar una paralización de 3 días.

Evalúe lo siguiente	Exponga sus comentarios
• **Confiabilidad en TI** Evalúe los siguientes factores: - La complejidad de los sistemas de información y el nivel de documentación existente. - La integración de los sistemas de información y el uso de sistemas de información aislados por los usuarios. - La Intervención manual para completar la información. - El uso de sistemas de información de tecnología obsoleta.	Los sistemas de información no se encuentran documentados. Observamos ausencia de habilidades en el personal de la Oficina de Informática y Estadística. La Universidad presenta sistemas aislados, que utilizan los mismos documentos fuentes.
• **Cambios en la tecnología de la Información:** Evalúe lo siguiente: - Los principales proyectos de automatización - El desarrollo o adquisición de sistemas de información considerando las necesidades de automatización de la Entidad. - El uso de nueva tecnología de información en reemplazo de tecnología obsoleta recibida de gestiones anteriores. - Los cambios a los procesos de negocio de la Entidad. (Anote que esto es alcanzado obteniendo un entendimiento del hardware, software y personal actual y planificado de la Entidad).	No se tiene confianza en el trabajo efectuado por el personal de esta Oficina Outsourcing de sistemas no se tiene actualmente en el área académica en el área administrativa se tienen los softwares generados por MEF y la SBS.

ADMINISTRACIÓN DE RECURSOS EN EL AREA DE SISTEMAS

Cuadro N°: 2 **Entidad:** Universidad Nac.Hermilio Valdizán **Auditor encargado:** Ing.Guadalupe Ramírez **Auditor revisor:** _____	**Hoja N°:**_____ **de** _____ **Año auditado: Diciembre / 2001** **Fecha: Enero 2002** **Fecha:** _____ / _____

Objetivo:	**Indique referencias**	**Exponga Comentarios**
Asegurar que la Entidad utiliza tecnología de información bajo criterios de costo-beneficio, considera las necesidades de automatización y adecuación a cambios del entorno en que se desenvuelve.		Como resultado de nuestra revisión de los controles relacionados con la administración de recursos realizada por el Área de Sistemas, consideramos que estos son insuficientes y requieren mejorarse para evitar mayores riesgos
Planes Estratégicos de Sistemas **1. Evalúe si la Entidad ha elaborado un Plan Estratégico de Sistemas, que determine la orientación para los próximos años.** **Evalúe lo siguiente:** • Que sea parte de la estrategia general de la Entidad • Que abarque todos los temas de la estrategia de la Entidad • Se encuentre actualizado y aprobado • Indique el nivel y calidad del personal involucrado • Haya sido aprobado por la Alta Dirección • Involucre el uso de tecnología emergente • Establezca el alcance, por ejemplo, áreas usuarias que participan, etc.		• La Oficina de Informática y Estadística de la Universidad no ha elaborado un Plan de Sistemas o un Plan de Trabajo que oriente las actividades de personal y que considere las necesidades de automatización de las facultades. • El último plan de trabajo fue preparado hace más de 3 años, y solo para un corto período de tiempo. • Las autoridades de la universidad no se involucran en temas de sistemas y ocasiona que no se pueda atender a tiempo los requerimientos existentes. • Las tecnologías emergentes no se utilizan por falta de planificación de las actividades.

Administración de recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Planeación y Administración de TI 2. Evalúe si la Alta Dirección y otros funcionarios de la Entidad se involucran en temas relacionados con sistemas **Evalúe lo siguiente:** • El grado de participación de la Alta Dirección • Se realiza una revisión de las variaciones de costo-beneficio • Se preparan presupuestos destinados a la ejecución • Se tiene conformado un Comité de Sistemas • Existe comunicación formal de la estrategia de sistemas • Se tiene la representación de todas las áreas usuarias de la Entidad • Se haya establecido la periodicidad en la emisión de informes comparada con la estrategia diseñada • Los términos de referencia se encuentran aprobados		• El Rectorado de la Universidad aún no se involucra y asume que los asuntos relacionados con la mejora de la eficiencia y efectividad de los principales procesos de negocio de la Universidad deben tener soporte en sistemas y tecnología. • La infraestructura tecnológica de la Universidad no ha sido renovada en los últimos 3 años y no se ha considerado como una necesidad estratégica realizar esta mejora. • La ausencia de una gerencia efectiva de la Oficina de Informática y Estadística está impidiendo que los objetivos y estrategias sean preparados y puestos de conocimiento de Rectorado

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Políticas y procedimientos de sistemas 3. Evalúe la existencia de políticas y procedimientos formales para administrar los recursos de sistemas **Evalúe lo siguiente:** • Que hayan sido aprobados por la Alta Dirección • Que establezca los objetivos de control, el alcance y la cobertura • Se hayan definido las responsabilidades • Se haya asignado la responsabilidad por el monitoreo o actualización • Haya sido distribuido al personal • Incluya asuntos con respecto a privacidad y derechos de autor. • Considere criterios de confidencialidad y seguridad de la información.		• No se han documentado, aprobado y difundido políticas, estándares y procedimientos relacionados con las actividades de personal que labora en la Oficina de Informática y Estadística. • Las actividades del personal se realizan de acuerdo al conocimiento y experiencia de cada persona y no se aplican criterios uniformes que establezcan criterios de control. • Incidentes de seguridad se han presentado debido a la ausencia de lineamientos específicos para la seguridad de la información generada en la Universidad.

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Asistencia a las áreas usuarias de la Entidad 4. Evalúe si existe asistencia a los usuarios que laboran en la Entidad respecto al uso de los recursos de sistemas **Evalúe lo siguiente:** • La existencia de políticas y procedimientos con respecto a asistencia a usuarios • Se tiene control de las licencias de derechos de autor de los programas • Se mantiene en uso programas estándares • Existen procedimientos para combatir los virus • Se tienen controles de seguridad • Se ha distribuido al personal • Se utilizan generadores de informes		• Existe ausencia de políticas, estándares y procedimientos que guíen las actividades de los usuarios respecto al uso adecuado de los recursos de cómputo de la Universidad. • Los usuarios desconocen como utilizar de forma efectiva los recursos de cómputo asignados. • Existen usuarios que han instalado programas ajenos a las labores propias de la Universidad y sin tener autorización de la Oficina de Informática y Estadística

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Unidad de Control Interno 5. Evalúe si la Unidad de Control Interno de la Entidad participa activamente en los desarrollos y operaciones de sistemas. **Evalúe lo siguiente:** • Si se han elaborado los términos de referencia de la participación • Se ha preparado un organigrama formal • Existe independencia en los trabajos efectuados • El personal que participa tiene conocimiento de temas de sistemas • Se tiene entrenamiento o experiencia en sistemas • Existe cobertura y enfoque en las áreas de sistemas • La revisión de sistemas es integral • Acción que se toma sobre los hallazgos es oportuna		• La Oficina de Auditoría Interna de la Universidad no participa en las actividades desarrolladas por la Oficina de Informática y Estadística al considerar que no es una de sus funciones. • Este personal desconoce temas de sistemas debido a que su formación académica está relacionada con la contabilidad y administración. • No se han programado cursos de capacitación para proveer al personal que labora en Auditoría Interna de las herramientas necesarias para hacer revisiones de sistemas

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Conciencia del Control en la Entidad 6. Evalúe si la actitud de la Alta Dirección de la Entidad propicia el control en las actividades efectuadas **Evalúe lo siguiente:** • Se realiza una evaluación del riesgo de sistemas informáticos • Se tiene en consideración asuntos de control en nuevos sistemas • Se manejan brechas en la seguridad • La responsabilidad sobre la seguridad ha sido asignada		• Observamos que al no haberse realizado un diagnóstico general de la Universidad y no tener un plan de mejoramiento para los problemas existentes, el Rectorado no está controlando de forma eficiente los recursos de la Universidad y no propicia una estructura de control interno apropiada

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Protección de Información de las áreas usuarias 7. Evalúe si la Entidad ha normado el uso y protección de información en medios seguros **Evalúe lo siguiente:** • El cumplimiento de la Entidad • El tipo y volumen de información protegida • Se establecieron requisitos futuros • Existen políticas establecidas por escrito		• La Universidad aún no ha normado el uso y protección de la información utilizada y mantenida en medios magnéticos, lo cual ocasiona incertidumbre y riesgo de acceso no autorizado.
Personal de Sistemas de la Entidad 8. Evalúe la existencia de políticas para contratar a personal de sistemas para laborar en la Entidad **Evalúe lo siguiente:** • La existencia de una política de contratación • La evaluación de experiencia y habilidades • Se otorga goce de vacaciones y horas extras • Se realizan evaluaciones de desempeño • Existen procedimientos de despido • Se provee entrenamiento de usuarios • Existe dependencia en personas claves • Se han establecido políticas y procedimientos de promoción de personal		• La contratación de personal para la Oficina de Informática y Estadística se realiza a través de concurso publico de méritos • No se realizan evaluaciones de desempeño y no ha habido capacitación al personal en los últimos 3 años. • No se dispone de personal especializado necesario para la gestión adecuada de la información de la Universidad, cuyo volumen es relativamente considerable

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Subcontratación de empresas externas 9. Evalúe si la Entidad ha establecido procedimientos para administrar trabajos realizados por terceros **Evalúe lo siguiente:** • Existen acuerdos contractuales formales • Se evalúa el desempeño de acuerdo al servicio • Existen controles de seguridad • Existen cláusulas de confidencialidad • Se hace revisión de fijación de precios por el servicio • Existen nivel de dependencia y conocimiento de la junta directiva • Se realizan auditorias		• No se tiene contrato con empresas externas para labores de mantenimiento preventivo y correctivo de equipos, por lo que cual no se puede evaluar esta actividad.
Inversión en sistemas 10. Evalúe si la Entidad ha preparado procedimientos que garanticen la inversión apropiada en sistemas **Evalúe lo siguiente:** • Existe una política para capitalizar / registrar los gastos • Existe un proceso de costeo formal • Se realiza revisión con los cambios y desembolsos que se anticipen • Se han considerado los cambios potenciales • Se ha evaluado el impacto de nueva tecnología		• La Oficina de Informática y Estadística no ha elaborado un presupuesto relacionado con las principales adquisiciones a efectuar durante el presente año.

Administración de Recursos en el Área de Sistemas	Indique referencias	Exponga Comentarios
Seguro contra todo riesgo 11. Evalúe si la principal infraestructura de cómputo se encuentra protegida **Evalúe lo siguiente:** • Se han incluido todos los equipos de cómputo de la Entidad • Se ha considerado los casos de pérdida de utilidades e incremento del costo del trabajo • Se han considerado los costos de recuperación • Fraude / confidencialidad • Requisitos de seguro sobre el negocio (o sea, estipulaciones de la póliza)		• La Universidad no mantiene una cobertura de seguros con alguna empresa especializada, por lo que existe el riesgo de pérdida de activos importantes de la Institución que no podrían ser recuperados.
Aspectos legales y regulados en la Entidad 12. Evalúe si la Entidad ha preparado procedimientos para cumplir con las regulaciones propias de su entorno de desarrollo institucional **Evalúe lo siguiente:** • Existencia de requisitos fiscales o normativos • Existencia de requisitos de privacidad • Cumplimiento de derechos de autor • Otras regulaciones • Evidencia de cumplimiento		• La Universidad guía sus acciones de acuerdo a lo establecido por la Asamblea Nacional de Rectores, preparando los reportes requeridos y atendiendo las consultas continuas. • Así mismo al MEF y SBS y eventualmente cuando el caso amerite a la CGR respecto a Sw legal.
Proyectos de Sistemas en la Entidad 13. Evalúe lo siguiente: • Verifique el uso de una metodología de administración de proyectos • Revise las políticas y procedimientos • Documente las técnicas de planeación • Revise el control del proyecto		• A la fecha de nuestra revisión, no se tienen proyectos de sistemas en ejecución debido a la falta de liderazgo e identificación específica de necesidades de automatización.

SEGREGACIÓN DE FUNCIONES EN EL AREA DE SISTEMAS

Cuadro Nº 3 **Entidad:** Universidad Nac.Hermilio Valdizán **Auditor encargado:** Ing. Guadalupe Ramírez **Auditor revisor:** _____	**Hoja N° _____ de _____** **Año auditado: Diciembre / 2001** **Fecha: Enero / 2002** **Fecha:** _____

Objetivo:	**Indique referencias**	**Exponga Comentarios**
Garantizar que exista una segregación razonable de las funciones del personal, tanto dentro del Área de Sistemas como entre las funciones de sistemas y de los usuarios, para prevenir y/o detectar errores o irregularidades.		Como resultado de nuestra revisión de los controles relacionados con la segregación de funciones del Área de Sistemas, consideramos que estos son insuficientes y requieren mejorarse para evitar mayores riesgos.
Estructura de la Organización del Área de Sistemas 1. Evalúe la estructura de la organización de Área de Sistemas **Evalúe lo siguiente:** • El nivel de reporte de los informes del Área de Sistemas • El tamaño de las operaciones en comparación con las necesidades de la Entidad		• Se tienen una estructura formal de la Oficina de Informática y Estadística dentro de la Universidad, pero el nivel de reporte no es apropiado para lograr el uso oportuno de las tecnologías.

Segregación de Funciones en el Área de Sistemas	Indique referencias	Exponga Comentarios
Segregación de Funciones–Sistemas 2. Evalúe la segregación de funciones dentro del Área de Sistemas de la Entidad, considerando su tamaño de organización. **Evalúe lo siguiente:** • Analice la segregación de funciones, por ejemplo:. - Número de miembros del personal de sistemas - Programadores de sistemas - Programadores de aplicaciones - Administración de la base de datos - Operaciones de TI - Ingreso de datos - Operaciones de redes - Seguridad • Analice la confiabilidad en el personal clave • Analice la confiabilidad en el personal bajo contrato • Determine la segregación de la administración de usuarios		• Se mantiene segregación de funciones entre las posiciones de analista de sistemas, programador de sistemas, operador de sistemas, estadístico y especialista administrativo. • Se han documentado las funciones de personal que labora en esta Oficina. • El personal que labora en esta Oficina es considerado clave dentro del proceso de gestión de la Universidad • Mantiene personal contratado en número de 2, con una antigüedad de 5 años y su vínculo es formal con la Entidad, considerados personal confiable, pero insuficiente para el área de sistemas; de los cuales sólo 1 está capacitado en sistemas.

Segregación de Funciones en el Área de Sistemas	Indique referencias	Exponga Comentarios
Segregación de Usuarios/Sistemas 3. Evalúe la limitación de responsabilidades de personal del Área de Sistemas de la Entidad **Evalúe lo siguiente:** • Analice la segregación de la administración de usuarios • Evalúe el acceso a contraseñas maestras • Determine la responsabilidad de iniciar o autorizar transacciones • Determine la custodia de los activos valiosos o móviles • Evalúe las modificaciones a los archivos maestros y otros datos • Analice la corrección de los errores en los datos de ingreso • Analice las pistas y revisión de auditoria		• El personal que labora en la Oficina de Informática y Estadística interviene en las labores de los usuarios cuando estos no se encuentran disponibles. • Dicho personal realiza ingreso, modificación y eliminación de datos de los sistemas más importantes de la Universidad sin dejar evidencia del requerimiento, autorización y cambios efectuados a los datos. • Los usuarios que piden el apoyo no revisan los cambios efectuados para conciliar los resultados y evitar algún error en el proceso.

SEGURIDAD DE INFORMACIÓN EN LA INSTITUCIÓN

Cuadro N° 4	**Hoja N° _____ de _____**
Entidad: Universidad Nac.Hermilio Valdizán	**Año auditado: Diciembre / 2001**
Auditor encargado: Ing. Guadalupe Ramírez	**Fecha: Enero / 2002**
Auditor revisor: _____	**Fecha:** _____

Objetivo:	**Indique referencias**	**Exponga Comentarios**
• **Garantizar que no pueda obtenerse acceso no autorizado a datos o programas confidenciales de la Entidad.** • **Garantizar que el ambiente en el que los sistemas funcionan protege su confidencialidad, integridad y confiabilidad.**		Como resultado de nuestra revisión de los controles relacionados con la seguridad de información en la Universidad, consideramos que estos son insuficientes y requieren mejorarse para evitar mayores riesgos.
Identificación de datos y aplicaciones confidenciales de la Entidad 1. Evalúe los procedimientos de la Entidad para proteger los datos y aplicaciones confidenciales **Evalúe lo siguiente:** • La existencia de una política de seguridad • La revisión de datos críticos durante el desarrollo • El proceso de evaluación de riesgos • El sistema de clasificación de datos		• La Universidad no tiene procedimientos formales para proteger la información académica y administrativa, lo cual le genera el riesgo de acceso no autorizado. • La Oficina de Informática y Estadística no ha preparado lineamientos relacionados con la seguridad de información

Seguridad de Información en la Institución	Indique referencias	Exponga Comentarios
Controles Detectores de Acceso 2. Evalúe los controles para identificar los accesos no autorizados y potenciales problemas de seguridad y hacer un seguimiento adecuado? **Evalúe lo siguiente:** • El monitoreo y vigilancia de los registros • Que el propietario de los datos compruebe regularmente los usuarios activos y los derechos de acceso de los usuarios		• En la organización de la Oficina de Informática y Estadística no ha sido considerado la posición de un especialista que se encargue de vigilar la seguridad de información e intentos de accesos no autorizados a la información académica y administrativa. • No se han definido los propietarios formales de la información de la Universidad.
Restricciones del Acceso a Usuarios – efectividad 3. Evalúe las medidas de seguridad diseñadas por el Área de Sistemas. **Evalúe lo siguiente:** • Se realiza el cambio periódico de contraseñas • Se utiliza una longitud para las contraseñas • Existe protección de las contraseñas • Existen procedimientos de despido de personal con contraseñas de importancia • Se preparan informes sobre violaciones de seguridad		• Para el control de acceso a la red y sistemas de información no se ha considerado medidas de cambio periódico de contraseñas; los usuarios pueden utilizar contraseñas de longitud corta; entre los usuarios no existe conciencia de protección de sus contraseñas compartiéndolas en la oficina; y cuando se equivocan al intentar ingresar a la red o sistemas, no informan a la Oficina de Informática.

Seguridad de Información en la Institución	Indique referencias	Exponga Comentarios
Acceso de personal de sistemas 4. Evalúe la existencia de controles que prevengan que el personal de sistemas acceda a los datos y programas de ambiente de producción. **Evalúe lo siguiente:** • Existen ambientes separados para producción y pruebas • Existen procedimientos para cambios de emergencia, - documentación actualizada - revisión periódica		• Los analistas y programadores no tienen restricciones para acceder a los directorios del ambiente de producción para efectuar cambios y actualizar programas, ocasionando que en muchas ocasiones se presenten errores en las áreas usuarias al no haberse probado lo suficiente dichos cambios.
Acceso Remoto a la Entidad 5. Evalúe los procedimientos de la Entidad para otorgar acceso remoto a otras instituciones públicas. Evalúe lo siguiente: • Existe control de acceso remoto por proveedores de servicio • Existe control de acceso remoto de los usuarios • Existe control de acceso remoto del personal de sistemas		• No se tienen comunicaciones especiales con otras Instituciones, que no sea a través del correo electrónico.
Control sobre contraseñas maestras y uso de programas utilitarios 6. Evalúe si se tiene control de la asignación, autorización y uso de identificaciones o contraseñas maestras **Evalúe lo siguiente:** • Número de personas que tienen acceso • Nivel de acceso de los usuarios • Controles de protección compensatorios (ejm., controles de acceso) • Emisión de informes sobre las actividades		• La contraseña de Administrador de la red es de conocimiento de todo el personal de la Oficina de Informática y Estadística, no habiéndose limitado solo a una persona dentro del área • Los usuarios tienen niveles de acceso de acuerdo a la función realizada dentro de la Universidad.

CONTROL DE ACCESO FÍSICO AL ÁREA DE SISTEMAS

Cuadro Nº 5	**Hoja Nº _____ de _____**
Entidad: Universidad Nac.Hermilio Valdizán	**Año auditado: Diciembre / 2001**
Auditor encargado: Ing. Guadalupe Ramírez	**Fecha: Enero / 2002**
Auditor revisor: _____	**Fecha:** _____

Objetivo:	**Indique referencias**	**Exponga Comentarios**
Garantizar la reducción al mínimo del riesgo de que ocurran daños accidentales o intencionales al equipo o los medios de computadoras, o el robo de ellos.		Como resultado de nuestra revisión de los controles relacionados con el control de acceso físico a la Oficina de Informática de la Universidad, consideramos que estos son insuficientes y requieren mejorarse para evitar mayores riesgos.
Seguridad Física 1. Evalúe si existe seguridad física adecuada con respecto al equipo de computadoras y los correspondientes datos, medios y documentación **Evalúe lo siguiente:** • Los edificios (incluso la protección de las terminales) • La sala de las computadoras • El equipo de comunicación • El almacenamiento a prueba de incendios para los medios magnéticos • La prevención o detección de incendios • El almacenamiento externo a la localidad • La protección ambiental • La continuidad de la electricidad • La protección de los cables de la red		• La Oficina de Informática y Estadística se encuentra ubicada en las oficinas administrativas de Rectorado y su acceso es restringido solo a personal autorizado. Este ambiente no tiene medidas de protección apropiada, permaneciendo la puerta abierta durante el día.

Control de Acceso Físico al Área de Sistemas	Indique referencias	Exponga Comentarios
Acceso a las instalaciones 2. Evalúe si existen medidas de control para garantizar que sólo los miembros del personal o los visitantes autorizados entren a las instalaciones **Evalúe lo siguiente:** • El requerimiento que el personal y los visitantes porten distintivos visibles de identificación • Los procedimientos que controlen la emisión de pases o distintivos a los visitantes • El requerir a los visitantes que estén acompañados de un miembro permanente del personal • Que el personal esté consciente de la seguridad, o sea, que confronten a los visitantes que no estén acompañados		• A la Oficina de Informática accede el personal que labora en esta área y algunas autoridades de la Universidad. • No se entrega fotochecks a los visitantes que acuden a la Oficina, por lo que este control no es apropiado. • No se acompaña a los visitantes al ingresar y salir de las Oficinas de Informática
3. Evalúe si existen controles para reducir el riesgo de robo del equipo y los medios **Evalúe lo siguiente:** • La autoridad que se requiere para retirar equipo de las instalaciones • La instalación de códigos de barra en el equipo • Los equipos sensores • La revisión de portafolios, bolsas		• Se tiene control mínimo al ingreso y salida de equipos de cómputo de la Universidad • El inventario de los equipos de cómputo instalados en la Universidad no están actualizados ni completos.

Control de Acceso Físico al Área de Sistemas	Indique referencias	Exponga Comentarios
Acceso a la sala de las computadoras 4. Evalúe si está restringido el acceso a los salones de las computadoras sólo a personas autorizadas Evalúe lo siguiente: • Un registro de visitantes (incluso ingenieros de sistemas, encargados de la limpieza, etc.) • El uso de equipos de control de acceso (ejm. tarjetas-clave) • Los controles para prevenir el uso erróneo del sistema de acceso por tarjeta - diferentes niveles de acceso - asignación de tarjetas - registro de infracciones - investigación de las infracciones • Las restricciones de acceso a diferentes áreas • El requisito de que los visitantes estén acompañados		• No se tiene sala de computadoras dentro de la Oficina de Informática.
Acceso a áreas restringidas 5. Evalúe si está más restringido el acceso a áreas que sean especialmente sensibles, tal como el área de telecomunicaciones **Evalúe lo siguiente:** • Los procedimientos de autorización de acceso • El registro de acceso • La revisión del registro de acceso		• No se tiene un área de telecomunicaciones dentro de la Oficina de Informática.

Control de Acceso Físico al Área de Sistemas	Indique referencias	Exponga Comentarios
Protección de las comunicaciones 6. Evalúe si existen controles para prevenir la pérdida o interrupción de las comunicaciones **Evalúe lo siguiente:** • Los canales seguros para los cables • El salón de servidores y central de comunicaciones bajo llave		• No se tienen instalaciones relacionadas con centrales telefónicas y equipos de comunicaciones.
Acceso de personal externo autorizado 7. Evalúe si está adecuadamente restringido el acceso de personal externo autorizado **Evalúe lo siguiente:** • Coordinar, autorizar y vigilar a los visitantes encargados de servicio y mantenimiento • Que el equipo de limpieza y el personal de servicio firme un registro al entrar y salir del edificio y las áreas de computadoras • Que se acompañe al equipo de limpieza / otros en el área de las computadoras		• No hay coordinaciones para evitar el acceso de personal ajeno a las labores de sistemas de la Universidad.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Cuadro Nº 6 **Entidad:** Universidad Nac.Hermilio Valdizán **Auditor encargado:** Ing. Guadalupe Ramírez **Auditor revisor:** _____	**Hoja Nº** _____ **de** _____ **Año auditado: Diciembre / 2001** **Fecha: Enero / 2002** **Fecha:** _____

Objetivo:	**Indique referencias**	**Exponga Comentarios**
Garantizar que los sistemas estén disponibles cuando se necesiten, que funcionen debidamente, que sean confiables, controlables y de costo beneficio, que tengan controles estrictos sobre la integridad de los datos y que satisfagan las necesidades de los usuarios		Como resultado de nuestra revisión de los controles relacionados con el desarrollo y mantenimiento de sistemas realizado por el Área de Sistemas, consideramos que estos son insuficientes y requieren mejorarse para evitar mayores riesgos.
Sistemas internos y/o modificaciones 1. Evalúe la metodología de desarrollo de sistemas utilizada por el Área de Sistemas. **Evalúe lo siguiente:** • Indique la metodología utilizada • Confidencialidad, integridad, disponibilidad, control y facilidad para auditar están incorporados en la metodología de desarrollo utilizada • Incluye procedimientos internos desarrollados por el equipo de desarrollo de sistemas • Se utilizan programas prototipos • Existen normas de programación		• En la Oficina de Informática y Estadística no se ha elaborado una metodología de desarrollo de sistemas. Las actividades de desarrollo y mantenimiento de sistemas son realizadas con base a los conocimientos y experiencia de los analistas y programadores de sistemas y usualmente no se documenta los trabajos asignados, no manteniéndose estándares de programación.

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Respaldo de programas adquiridos a empresas externas 2. Evalúe si el personal de sistemas da mantenimiento continuo a los programas. **Evalúe lo siguiente:** • Existe un contrato de mantenimiento con el proveedor • Se realiza verificación y pruebas de los cambios y mejoras antes de su instalación • Se ha obtenido el código fuente • Se tienen medidas para prevenir el acceso no autorizado a los programas • En cuanto al proveedor de programas: cantidad de personal de respaldo, referencias, confiabilidad • Se tienen contratos actualizados • Se realiza certificación de los programas • Se evalúan las implicaciones de las modificaciones internas • Los sistemas de información son estables		• El personal de sistemas realiza los cambios y modificaciones requeridos por los usuarios de las áreas académicas y administrativas. • Los sistemas de información que provienen de otras entidades no son modificados por este personal, y sólo se coordina su actualización periódica. • Los sistemas de información relacionados con el proceso académico no son estables y se requiere mucha labor para hacerlos operar normalmente, originando reclamos continuos de los usuarios del área y alumnos
Desarrollo y/o mantenimiento de terceros 3. Evalúe los estudios de costo y beneficio de los trabajos realizados con el apoyo de empresas externas **Evalúe lo siguiente:** • Se tiene una administración de los costos • Se evalúa la reputación de proveedor • Se evalúa la calidad del personal • Se mantienen normas de programación • Existen antecedentes de la empresa		• No se realizan trabajos con empresas externas.

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Revisión de Proyectos por la Gerencia 4. Evalúe si la Alta Dirección revisa los avances en los trabajos de desarrollo y cambio a los sistemas así como los costos relacionados. **Evalúe lo siguiente:** • La periodicidad de emisión de informes a la alta gerencia • El control de los presupuestos • Los métodos de costos • El monitoreo del proceso • Todos los costos sean incluidos		• El Rectorado no interviene en los desarrollos y cambio a los sistemas de información. • La jefatura de informática no emite informes al Rectorado indicando el grado de avance de los trabajos asignados.
Restricción de Transferencias a Producción 5. Evalúe la limitación para instalar nuevas versiones en el ambiente de producción. **Evalúe lo siguiente:** • Se mantiene controles de acceso • Que el personal de desarrollo no pueda trasladar los programas a producción • Se registran pistas de auditoria de los pases de programas		• Los analistas y programadores no tienen restricciones para instalar los cambios al ambiente de producción. • Los cambios a los programas no son documentados y no se puede evaluar el nivel de aprobación obtenido.
Documentación 6. Evalúe la documentación de los sistemas de información. **Evalúe lo siguiente:** • Se mantiene una descripción de los objetivos de los sistemas • Se da cumplimiento de normas de programación • Se mantiene documentación del sistema • Existen instrucciones de operación • Existe documentación de usuarios		• Los analistas y programadores no han preparado documentación técnica y de usuario de los trabajos realizados. • Los cambios a los programas y archivos de datos se realizan de acuerdo a la experiencia del personal sin tener en cuenta normas y estándares de programación.

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Procedimientos de Control de Cambios 7. Evalúe si se mantienen procedimientos apropiados para autorizar y documentar la iniciación y traslados a producción de los cambios. **Evalúe lo siguiente:** • Se tienen procedimientos para aprobar las solicitudes de los usuarios • Se tiene políticas de documentación • Se mantiene documentación de los cambios a los programas • Se requiere la autorización de la Jefatura • Se mantiene un registro de los cambios (generales y detallados) y antecedentes del programa		• Los procedimientos relacionados con la atención de requerimientos, asignación de trabajos y el pase de programas de desarrollo a producción aún se han documentado.
Pruebas de Cambio 8. Evalúe la existencia de las pruebas de los cambios por los que los desarrollan y por los usuarios **Evalúe lo siguiente:** • Se tienen procedimientos de prueba • Se logra la participación de los usuarios en la autorización y la prueba de los cambios • Se obtienen pruebas completas y apropiadas • Se mantienen pruebas debidamente documentadas y analizadas		• Las pruebas efectuadas son informales y realizadas por los analistas y programadores sin la participación de los usuarios. • No se han documentado procedimientos de prueba de cambios y desarrollos. • En caso de revisión posterior, se tendría que acudir a la persona que realizó el trabajo para obtener detalles específicos.

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Cambios de Emergencia 9. Evalúe los procedimientos establecidos para controlar cualquier cambio de emergencia que efectúe el personal de desarrollo de sistemas **Evalúe lo siguiente:** • Se obtiene la aprobación del operador de sistemas • Se mantiene registro de todos los cambios de emergencia • Se realizan pruebas • Se obtiene la aprobación posterior de la Alta Dirección, del J • efe de Sistemas, según corresponda		• No se han documentado procedimientos para cambios de emergencia.
Segregación de Pruebas y Producción 10. Evalúe si se asignan bibliotecas por separado para las pruebas de desarrollo y las actividades de producción **Evalúe lo siguiente:** • Se mantiene una segregación de bibliotecas de desarrollo / pruebas de aceptación / producción • Se tienen procedimientos / restricciones de transferencias / traslados		• Se tiene ambientes separados en los servidores de red para realizar las labores de desarrollo y poner en producción los programas desarrollados o cambiados. • Los procedimientos para realizar estas actividades no han sido documentados.
Aprobación de los sistemas probados 11. Evalúe si se requiere una aprobación formal después de efectuar pruebas del sistema. **Evalúe lo siguiente:** • La oportunidad de la aprobación (por ejemplo, antes de trasladar a producción) • La autoridad del individuo que efectúe la aprobación		• La aprobación formal de los usuarios nunca se requiere, debido a que los analistas y programadores realizan esta actividad.

Desarrollo y Mantenimiento de Sistemas	Indique referencias	Exponga Comentarios
Entrenamiento en los nuevos sistemas 12. Evalúe si reciben los usuarios un entrenamiento apropiado sobre las facilidades de los nuevos sistemas antes de la implantación. **Evalúe lo siguiente:** • Flujogramas del sistema • Diagramas de flujo de datos • Estructuras de datos lógicos • Diccionario de base de datos • Especificaciones del sistema • Especificaciones del programa • Almacenamiento externo de copias de la documentación esencial		• Los usuarios son capacitados en las nuevas opciones y reportes disponibles en los sistemas de información.

CONTINUIDAD DE SISTEMAS DE LA ENTIDAD

Cuadro N° 7 **Entidad:** Universidad Nac.Hermilio Valdizán **Auditor encargado:** Ing. Guadalupe Ramírez **Auditor revisor:** _____	**Hoja N°** _____ **de** _____ **Año auditado: Diciembre / 2001** **Fecha: Enero / 2002** **Fecha:** _____

Objetivo:	**Indique referencias**	**Exponga Comentarios**
Reducir al mínimo la posibilidad de que ocurra un desastre total y garantizar que el negocio pueda reanudar sus operaciones con efectividad (dentro de un período razonable de tiempo) en caso que ya no se disponga de las instalaciones de procesamiento existentes.		Como resultado de nuestra revisión de los controles relacionados con la continuidad de sistemas de la Universidad, consideramos que estos son insuficientes y requieren mejorarse para evitar mayores riesgos.
Evaluación de Riesgos–Interrupción de la Entidad 1. Evalúe si se han identificado las funciones y los sistemas críticos de la Entidad. **Evalúe lo siguiente:** • Funciones claves y períodos de tolerancia en cada caso • Que el plan de recuperación tome en cuenta los asuntos de negocio y de computadoras • Tiempo que el negocio funcionar con efectividad sin sus sistemas críticos de computadoras		• Las procesos académicos y administrativos son los más importantes para la Universidad, pero no se ha identificado los usuarios considerados clave, las funciones que ejecutarán en la recuperación y los tiempos mínimos requeridos.

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Continuidad de la Entidad 2. Evalúe si se ha documentado un plan de continuidad del negocio que sea apropiado **Evalúe lo siguiente:** • Revisión y actualización periódica del plan • Procedimientos de los usuarios. • Aprobación de la Alta Dirección. • Alcance, de los sistemas centrales y computación de usuarios; servicios internos y de terceros; TI e ingreso de datos de los usuarios		• No se ha documentado un plan de recuperación en caso de desastres, por lo que los procesos académicos y administrativos se verían afectados.
Procedimientos de recuperación 3. Evalúe si han especificado los usuarios sus requisitos de recuperación **Evalúe lo siguiente:** • Los niveles de interrupción • Recuperación de las aplicaciones críticas solamente • Recuperación de las aplicaciones • Procedimientos adicionales para el manejo del ingreso de datos, si fuese apropiado • Duración de los métodos provisionales de procesamiento		• Los usuarios no han especificado los requerimientos de recuperación y el orden de prioridad requeridos.
Métodos de trabajo provisionales 4. Evalúe si han desarrollado los usuarios métodos de trabajo provisionales (como parte de sus procedimientos de recuperación) para ponerlos en práctica en caso que se interrumpa el procesamiento normal		• Los usuarios no han documentado las actividades a ejecutar en caso de ausencia o indisponibilidad de los sistemas de información.

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Fortalecimiento del Local 5. Evalúe si se efectúan revisiones periódicas de los análisis de riesgo, como parte de un ejercicio para evitar desastres, para reducir al mínimo la posibilidad de que ocurra una interrupción total **Evalúe lo siguiente:** • El alcance de las revisiones • La fecha de la revisión más reciente • Las medidas tomadas		• No se realiza esta actividad.
Prevención y Reducción de Interrupciones 6. Evalúe si están los sistemas y las operaciones de negocios diseñados de una manera efectiva para reducir las interrupciones al mínimo **Evalúe lo siguiente:** • Protección contra intromisión no autorizada • Rutas alternas para las redes • Reemplazo de componentes • Respaldo ofrecido por los proveedores de los equipos • Mantenimiento preventivo		• Se requiere continuamente la participación de personal de sistemas para lograr que el sistema funcione correctamente.

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Frecuencia de los Respaldos 7. Evalúe si se hacen copias de respaldo de los archivos de datos y los programas y se almacenan dentro y fuera de la localidad con suficiente periodicidad **Evalúe lo siguiente:** • Oportunidad del respaldo • Frecuencia • Relación con el procesamiento / cambios críticos • Duración de los ciclos de los procesos principales • Volúmenes de datos comprarados con los respaldos almacenados externamente • Recuperabilidad de los documentos fuentes • Respaldos periódicos parciales comparados con respaldos completos		• Se hace copia de respaldo de forma irregular y no se mantiene información vital de los registros académicos e información administrativa protegida y guardada en lugar seguro.
Composición de los Respaldos 8. Evalúe si se respalda lo siguiente de manera apropiada: • Los archivos de datos • Los programas • Los programas de los sistemas • La documentación de los sistemas • Los procedimientos de operación • Los procedimientos de usuarios • Plan de Recuperación en Caso de Desastre		• Solo se obtiene copia semanal de algunos archivos de datos que no son críticos para la Universidad. • Los procedimientos de recuperación no están documentados.

Continuidad de Sistemas de la Entidad	Indique referencias	Exponga Comentarios
Respaldo de Seguridad / Localidad 9. Evalúe si se mantienen las copias de respaldo en una localidad segura tanto localmente como externa a donde se encuentran las computadoras **Evalúe lo siguiente:** • Registro de los traslados de los medios de almacenamiento • Autoridad para trasladar los medios • Lo apropiado de las localidades internas y externas de almacenamiento • Cómo se efectúan los respaldos para garantizar su recuperación		• Las copias se guardan en la Oficina de Informática y Estadística en un cajón de escritorio sin llave. • No se tienen copias de respaldo en lugar externo a la Universidad.
Pruebas de Recuperación 10. Evalúe si se someten a pruebas apropiadas los procedimientos de respaldo y de recuperación **Evalúe lo siguiente:** • El tiempo que toma recuperar • El procesamiento involucrado en la recuperación • Las pruebas efectuadas después de cambios al sistema y a los programas • La frecuencia de las pruebas • La fecha y el resultado de la última prueba • La efectividad de las pruebas • Medidas posteriores adoptadas • Los cambios en los programas del sistema que puedan impactar la recuperación		• No se ha realizado alguna actividad respecto a este tema.

CAPITULO VI

PRESENTACIÓN DE RESULTADOS DE LA APLICACIÓN DE LA AUDITORÍA

6.1. PRESENTACIÓN DEL INFORME DE AUDITORÍA INFORMÁTICA

A continuación se muestra un resumen de los principales hallazgos, el impacto de cada uno de ellos respecto al riesgo que representa para el funcionamiento de la entidad y el plazo de ejecución de las acciones que tendría que tomar la Universidad.

Para la determinación de los impactos se ha tomado en cuenta, que la Universidad tiene como macroproyecto la acreditación universitaria, por tanto el uso de tecnología de información debería estar orientado al logro de dicho objetivo estratégico. La acreditación universitaria exige entre otras cosas, que la institución sea moderna; es decir, que responda con velocidad y eficiencia ante cualquier cambio en el entorno, que los servicios que presta sean de calidad; entendiéndose por ello, que el servicio o producto responda a los requerimientos con eficiencia, eficacia, efectividad y competencia. Así mismo, es necesario que la institución sea evaluada mediante procesos de evaluación externa y autoevaluación en todos los aspectos, siendo importante la auditoría informática, para la identificación de riesgos y evaluación de controles en el uso de tecnología de información.

Es importante señalar además, que las situaciones observadas ocasionan a la Universidad pérdida de imagen, debido a la baja calidad de atención a los clientes, pérdidas monetarias por el uso excesivo de recursos humanos en procesos que podrían automatizarse, por reprocesos, duplicidad de procesos, inconsistencias, debido a procesos que no se encuentran estandarizados, etc.; pérdida de operatividad

porque podrían utilizarse con mayor eficiencia los recursos tecnológicos de información, etc.

El siguiente cuadro resume los hallazgos más importantes entregados a la Alta Dirección de la Universidad.

UNIVERSIDAD NACIONAL HERMILIO VALDIZAN

PRESENTACIÓN DE LOS PRINCIPALES HALLAZGOS, IMPACTO Y PLAZO DE ACCIONES A EJECUTAR

Control	Situación observada	Impacto	Plazo de Ejecución
Administración de recursos en el Área de Sistemas	1. Ausencia de un Plan de sistemas	Alto	Corto plazo
	2. Ausencia de políticas y procedimientos formales	Moderado	Mediano plazo
	3. Ausencia de procedimientos para los usuarios	Moderado	Mediano plazo
	4. Personal de sistemas sin adecuado entrenamiento	Alto	Corto plazo
	5. Participación limitada de Auditoria Interna	Alto	Corto plazo
	6. Ausencia de cobertura de seguros	Alto	Corto plazo
Segregación de funciones en el Área de Sistemas	7. Nivel de reporte de la Oficina de Informática no es apropiado	Alto	Corto plazo
	8. Personal de sistemas realiza labores de usuario final	Alto	Corto plazo
Control de acceso físico al Área de Sistemas	9.Accesos no autorizados a la Oficina de Informática	Moderado	Mediano plazo
	10. Oficina carece de medidas de protección física y ambiental	Alto	Corto plazo
Seguridad de información en la Universidad	11. No se ha establecido política de seguridad de información para la Universidad	Alto	Corto plazo
	12. No se tiene una persona a cargo de la administración de la seguridad de acceso	Alto	Corto plazo
	13. No se han establecido valores de seguridad adecuados en la red	Alto	Corto plazo
	14. Analistas y programadores tienen acceso a programas y datos del ambiente de producción	Alto	Corto plazo
	15. No se han definido los propietarios de la información de la Universidad	Alto	Corto plazo

	16. Contraseñas de alto nivel son conocidas por mas de una persona	Alto	Corto plazo
Desarrollo y mantenimiento de sistemas	17. No se ha desarrollado una metodología de desarrollo de sistemas de la Universidad	Moderado	Mediano plazo
	18. No se tienen documentación actualizada de los sistemas	Moderado	Mediano plazo
	19. Sistemas de información no son estables y ocasionan errores	Alto	Corto plazo
	20. No se documenta los trabajos efectuados por los analistas y programadores	Alto	Corto plazo
Continuidad de sistemas de la Universidad	21. No se ha preparado una evaluación de los riesgos asociados con sistemas	Alto	Corto plazo
	22. No se ha documentado un plan de contingencia ante desastres	Alto	Corto plazo
	23. No se han documentado los métodos de trabajo alternativos de los usuarios	Moderado	Mediano plazo
	24. Obtención de copias de respaldo en periodos irregulares.	Alto	Corto plazo
	25. No se mantienes copias de respaldo en lugar seguro	Alto	Corto plazo

CAPÍTULO VII

CONCLUSIONES Y RECOMENDACIONES

7.1. CONCLUSIONES

1. 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.
2. El diseño de los cuestionarios, permite recopilar información acerca de las causas que motivaron al auditor a calificar el riesgo a un área, el mismo que sirve como punto de partida para posteriores auditorías.
3. Para el desarrollo de la metodología y el diseño de cuestionarios se tomó como fuente las referencias contenidas en el COBIT, las normas de Contraloría General de la República básicamente y otras normas de aceptación internacional, como las NIAS, NAGU, MAGU, etc.
4. La Auditoría Informática es un medio que dispone la Entidad Pública para evaluar los riesgos y controles en el uso de tecnología de información.
5. La Auditoría Informática permite a la Entidad Pública buscar los medios para alcanzar los estándares internacionales en el uso adecuado de las tecnologías de información, con miras a una certificación de calidad.
6. La Auditoría Informática 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 para la Entidad.

7. 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.
8. La aplicación de la Auditoría Informática en la Universidad Nacional Hermilio Valdizán de Huánuco, se ha realizado entre el 01 de diciembre del 2001 y enero del 2002.
9. El desarrollo de la metodología propuesta nos ha permitido determinar los niveles de riesgo y control en el uso de la tecnología de información en la Universidad Nacional Hermilio Valdizán de Huánuco, cuyos resultados más importantes están orientados a mejorar las áreas de administración de tecnología de información, segregación de funciones, seguridad de la información, desarrollo de sistemas y continuidad de sistemas.
10. Se han detectado 25 hallazgos de importancia. El 76% de los mismos son de impacto alto, mientras que el 24% son de impacto moderado.

7.2. RECOMENDACIONES

1. El registro de las causas que motivaron la calificación de los riesgos y controles, es una buena práctica que debe mantenerse en los procesos de auditoría, los que servirán para que las personas responsables de las áreas de informática de las Entidades conozcan los riesgos y efectos que los mismos pueden generar en la institución, de persistir con ellos en el tiempo.
2. El registro de parte de los auditores de las causas que motivaron una determinada calificación permitirán un conocimiento rápido de la situación que las generaron y servirá de punto de partida para auditorías futuras y durante los procesos de seguimiento de la auditoría.
3. Se recomienda el uso de la Auditoría Informática como una herramienta de gestión de la Entidad, la misma que permitirá administrar adecuadamente los recursos de tecnología de la información, buscando obtener los mejores niveles de seguridad, confiabilidad y continuidad, para el logro de ventajas competitivas de la Entidad.
4. La implementación de los controles requeridos para reducir el nivel de riesgo de impacto alto deben efectuarse de forma inmediata, por lo que recomendamos al Consejo Universitario prepare un Plan de Actividades para implementar las mejoras en las áreas identificadas.
5. Debe rediseñarse la organización del área de informática de la Universidad y reubicarse dentro de la estructura orgánica, de manera que participe efectivamente en el Planeamiento Estratégico de la Institución y cumpla con los dispuesto la Directiva Nº010-95-INEI/SJI, artículo 5.8., inciso b.
6. El responsable del área funcional a cargo de la gestión de tecnología y sistemas de información de la Universidad, debe elaborar al más breve plazo un Plan de Sistemas de Información y el Plan de Contingencias, tal como lo estipula las Normas Técnicas de Control Interno para el Sector Público, en el numeral 500-02 y 500-06.
7. La Institución debe brindar los recursos necesarios para implementar gradualmente las recomendaciones descritas en cada una de las observaciones realizadas durante el proceso de Auditoría Informática en la Universidad

Nacional Hermilio Valdizán de Huánuco, con la finalidad de controlar los riesgos que pueden afectar la continuidad de las operaciones de la Entidad, salvaguardar los activos y mejorar el uso eficiente de los recursos de tecnología de la información.

8. La institución debe planificar cursos de capacitación en el uso eficiente de los recursos de tecnología de la información tanto al personal del área de informática como de toda la institución.

BIBLIOGRAFÍA

1. BERNAL, Rafael y COLTELL, Simón. Auditoría de los Sistemas de Información. Universidad Politécnica de Valencia. 1997
2. CHECKLAND, Meter. Pensamiento de Sistemas, Práctica de Sistemas. Edit. Megabyte. México. 1993
3. DAGOBERTO PINILLA, José. Auditoria Informàtica. Aplicaciones en Producción. ECOE ediciones. Bogotá-Colombia. 1997
4. De, Miguel y PIATTINI, M. Fundamentos y modelos de bases de Datos. Editorial Ra-Ma. Madrid. 1997.
5. DERRIEN, Y. Técnicas de Auditoría Informática. Marcombo, Barcelona. 1994.
6. ECHENIQUE GARCÍA, José Antonio. Auditoría en Informática. Edit. Mc Graw Hill. 1995.
7. ESPINOZA, Sergio. Auditoría en Sistemas de Información: El Nuevo Concepto. Conferencia del Congreso Interamericano de Contaduría Pública "Reingeniería de la Contaduría ante los retos del Nuevo Milenio". 1997. San José de Costa Rica.
8. FERREYROS MORÓN, Juan A. Informática Contable y Auditoría de Sistemas. Edit. La Senda. Perú. 1995.
9. GONZÁLES ZUBIETA, José María. Metodologías de Control Interno, Seguridad y Auditoria Informàtica. Coautor de Auditoría Informática. Piattini. Pág. 45-91.
10. GIL PEUCHAN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Edit. McGraw Hill. Madrid-España. 1999

11. GÓMEZ MARÍN, Jacinto Oscar. Auditoría de Sistemas aplicado al Sector Público en el Instituto Peruano de Seguridad Social. Informe de Experiencia Profesional. Lima. 1999

12. HERNANDEZ GARCIA, Alonso. La Informática como Herramienta del Auditor Financiero. 1998. Coautor de Auditoría Informática. Piattini. Pág. 3-23.

13. HERNÁNDEZ, Roberto; FERNÁNDEZ, Carlos; BAPTISTA, Pilar. Metodología de la investigación. Edit. Mc Graw Hill, México 1998.

14. IBM del Perú. Control y Auditoría de Sistemas de Información. Departamento de Educación de IBM del Perú S.A. 1998.

15. IBM del Perú. Seguridad en Sistemas de Información. Departamento de Educación de IBM del Perú S.A. 1998.

16. INEI. Auditoría Informática. Publicación del Instituto Nacional de Estadística e Informática del Perú. 1996.

17. ISACA. Cobit. Guidelines Management http://www.isaca.org

18. LAMERE, J.M. La seguridad Informática. Metodología. Ediciones Arcadia. 1995.

19. LI, David. Auditoría en Centros de Cómputo. Edit. Trillas. Barcelona.1990

20. MILLS, David. Manual de auditoría de la Calidad. Ediciones Gestión 2000. Barcelona. 1997.

21. MURPHY, David. La auditoría de sistemas informáticos. Temas Avanzados. Documento hecho en la Escuela Nacional de Control. Contraloría General de la República. 1998.

22. NÚÑEZ PONCE, Julio. Derecho Informático. Edit. Marsol. Perú Editores S.A. 1996.

23. ORJEDA JIMENZ, Leonidas. Auditoría informática. Editorial Presencia Ltda.. 1992.

24. PIATTINI, Mario y Del Peso, Emilio. Auditoría Informática. Un enfoque práctico. Grupo editor Alfaomega. Colombia. 1998

25. SALKIND, Neil. Métodos de investigación. Prentice may. México. 1997.

26. TORRIN, M. La Auditoría Informática. Métodos, reglas, normas. Edit. Masson. Barcelona. 1989.

27. WILSON, Brian. Sistemas: Conceptos, metodología y aplicaciones. Editorial Limusa, México 1993.

28. ZORRILLA, Santiago; TORRES, Xamar; Guía para elaborar la tesis. Edit. Mc Graw Hill. México. 1992.

DIRECCIONES ELECTRÒNICAS

1. ACUF, Marshall, SMITH, Salomon. Information Security Impacting Securities Valuations. Agosto 2000. http://www.itaudit.org/index search.htm
2. BOXIO PEREZ, José Ignacio. Auditoría de Redes. 1999. http://www.oai.org/publi.htm
3. CARRILLO, Cristina, QUINTERO, Alejandro. Modelo de Coordinación de Sistemas Multiagentes Aplicado a quienes realizan la Labor de Auditoría de Sistemas de una Organización. acarrillo@uniandes.edu.co, aquinter@uniandes.edu.co
4. CODERRE, Dave. Ratio Análisis An Understated Data Análisis Technique. Abril 2001. dcoderre@cyberus.sa; http://www.itaudit.org/index search.htm
5. FOGGON, Keith The Artificial Auditor. Octubre 1999. keith.foggon@sapphire.net; http://www.itaudit.org/index search.htm
6. GABRIEL DESMONTS BASILIO. La Auditoría Física. 1999. http://www.oai.org/publi.htm
7. GARCIA SUELO, Manuel Palao. Auditoría Informática de EIS/DSS y Aplicaciones de Simulación. 1999. . http://www.oai.org/publi.htm
8. GAO. Information Tecnology Investment Management. http://wwwgao.gov
9. GOLDSMITH, Jim. Perform an audit. On the RACF Database. Junio 2000. Jim Goldsmith@VALIC.com; http://www.itaudit.org/index search.htm
10. GOMEZ VAZ, Manuel. Auditoría de la Ofimática. 1999. http://www.oia.org/public.htm
11. GRANJA ALVAREZ, Juan Carlos. Auditoría Informática en Proyectos Informáticos de Nuevas Tecnologías de Telefonía Móvil. Julio 2001. http://www-etsi2.ugr.es/planes/proyectos/lsi/2000-2001/lic/jcgrnl.phtml

12. GRIFFITHS, David. Auditing Mangemenet Information. April 2001. dmgriffiths@managing-information.org.uk; http://www.itaudit.org/index_search.htm

13. HUGH H, PENRI, Williams. Intrusion Prevention and Detection. Febrero 2001.Hugh.Penri-Williams@alcatel.fr http://www.itaudit.org/index_search.htm

14. INSTITUTE OF INTERNAL AUDITORS. INFORMATION SECURITY ASSURANCE: Board and Management Solutions. Conference. Mayo 2001. http://www.theiia.org/ecm/conferences.cfm?doc_jd=1764

15. LE GRAND, Charles H. Use of CAATS in audit. Management. Publicación en Internet. clegrand@theiia.org; http://www.itaudit.org/index_search.htm

16. LE GRAND, Charles and OZIER, Will. Information Security Management and Assurance: A call action. January 2000. clegrand@theiia.org; http://www.itaudit.org/index_search.htm

17. LE GRAND, Charles; LEY PARKER, Xenia; HORTON, Tomas. Information Security Governance. clegrand@theiia.org; http://www.itaudit.org/index_search.htm

18. LUCEROS MANRESA, José Luis. Auditoría de la Calidad. 1999. . http://www.seio.org/publi.htm

19. MADURGA OTEIZA, José María. Auditoría de Aplicaciones. 1999. . http://www.oai.org/publi.htm

20. MARTIN, Denys. Comparison of Principal Models for IT & C audit. Analysis (Part A). August 2001. http://www.itaudit.org/index_search.htm

21. OLIPHANT, Alan. IT Auditing Without Pain – The Internet, Part2: Making a Start. mair@mair-international.com; http://www.itaudit.org/index_search.htm

22. OZIER, Will. Information Risk Análisis, Assessment and Mangemenet. Febrero 2000. woozier@pacbell.net; http://www.itaudit.org/index_search.htm

23. PATHAK, j.p. Needed: A Policy Doctrine on Information Security in Developing Countries _ Part 1. Marzo 2000. pathakjp@goa1.dot.net.in; http://www.itaudit.org/index_search.htm

24. PATHAK, j.p. Needed: A Policy Doctrine on Information Security in Developing Countries _ Part 2. Abril 2000. pathakjp@goa1.dot.net.in; http://www.itaudit.org/index_search.htm

25. PRICE, Dick. A New Standard in Information Security management Part 2: An examination of detailed controls. Mayo 1999.

dickprice@cix.compulink.co.uk; http://www.itaudit.org/index_search.htm

26. YU, John. What auditors should know about e-appliances. Marzo 2000. jwyu@attglobal.net; http://www.itaudit.org/index_search.htm