UNIVERSIDAD CIENFUEGOS
Carlos Rafael Rodríguez

FACULTAD DE CIENCIAS ECONÓMICAS Y EMPRESARIALES

DEPARTAMENTO DE CIENCIAS CONTABLES

TEMA: CONTROL INTERNO

CONTRALORÍA PROVINCIAL CIENFUEGOS

TÍTULO: Guía metodológica para la evaluación del Sistema de Control Interno a las tecnologías de la información.

AUTORA: Lisbet Guerra Poma

TUTORES: MSc. Norma León López

Lic. José R. Méndez Terry

INSTITUCIÓN: CONTRALORÍA PROVINCIAL CIENFUEGOS.

CURSO 2011-2012

AVALES

Hago constar que el presente trabajo fue realizado en la Universidad de Cienfuegos “Carlos Rafael Rodríguez” como parte de la terminación de los estudios en la Especialidad de Licenciatura en Contabilidad y Finanzas, autorizando a que el mismo sea utilizado por las organizaciones e instituciones para los fines que estime conveniente. No podrá este trabajo ser presentado a eventos, ni publicado sin la aprobación del centro.

_____

Firma del AUTOR

Los que abajo firmamos, certificamos que el presente trabajo ha sido revisado según acuerdo de la Dirección de nuestro centro y que el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura, referido a la temática señalada.

_____	_____
Información Científico Técnica	Computación
Nombre, Apellidos y Firma	Nombre, Apellidos y Firma
_____	_____
Firma del TUTOR	Firma del TUTOR

PENSAMIENTO

La experiencia nos ha enseñado que aquello que no se controla con efectividad, no se cumple o se ejecuta superficialmente.

Raúl Castro Ruz, Enero 2012

DEDICATORIA

A mi Madre

Por ser la impulsora de mis acciones.

A mis Hijos

Leandro y Leonardo por ser la inspiración e ilusión de mi vida.

A mis hermanos

Por su cariño y comprensión.

A mi Esposo

Por ser mi gran compañero y guía.

Agradecimientos:

"Sentir gratitud y no expresarla es como
Envolver un regalo y no darlo."
William Arthur Ward

Quiero dejar constancia escrita, porque así no lo borra el tiempo, de mi eterno agradecimiento a toda las personas excelentes que me rodean, y que sin su ayuda no pudiera estar viviendo este momento…y también ¿por qué no? a la no tan buena que me da fuerzas para seguir…

A *mi madre y esposo*… por su apoyo incondicional, siempre pendientes de mí
A *toda mi familia*… siempre juntos en las buenas y en las malas
A *mis tutores*… por sus conocimientos, su paciencia, valentía y gran apoyo

En fin a todos aquellos que pusieron su confianza y dedicación en la confección de este trabajo…

Gracias

RESUMEN

Esta investigación presenta el diseño de una guía metodológica para la evaluación del Sistema de Control Interno a las tecnologías de la información, persiguiendo como objetivo: elaborar una guía metodológica que permita verificar el cumplimiento de lo establecido referente a los recursos de las tecnologías de la información y sus servicios asociados mejorando el sistema evaluación del control interno de los sistemas informáticos de las organizaciones, facilitando la aplicación adecuada de las técnicas de recolección de evidencias, y que a su vez permita profundizar en la revisión de los documentos, sistemas informáticos implementados en las organizaciones, asegurando que la evidencia recopilada sea suficiente y competente, y los resultados del examen, objetivos y concluyentes, que determinen el resultado, o sea, que permita realizar una evaluación del Sistema de Control Interno a las Tecnologías Informáticas; así como, optimizar el uso del tiempo de manera razonable en las acciones de control realizadas por los auditores del sistema.

Durante el desarrollo de la investigación se emplearon métodos, procedimientos y técnicas del nivel teórico y empírico, matemático y estadístico, para procesar información y validar la efectividad de la guía metodológica elaborada.

SUMMARY

This investigation presents the design of a methodological guide for the evaluation from the System of Internal Control to the technologies of the information, pursuing as objective: to elaborate a methodological guide that allows to verify the execution of that settled down with respect to the resources of the technologies of the information and their associate services improving the system evaluation of the internal control of the computer systems of the organizations, facilitating the appropriate application of the techniques of gathering of evidences, and that in turn it allows to deepen in the revision of the documents, computer systems implemented in the organizations, assuring that the gathered evidence is enough and competent, and the results of the exam, objectives and conclusive that determine the result, that is to say that allows to carry out an evaluation from the System of Internal Control to the Computer Technologies; as well as, to optimize the use of the time in a reasonable way in the control actions carried out by the auditors of the system.

During the development of the investigation methods were used, procedures and technical of the theoretical and empiric, mathematical and statistical level, to process information and to validate the effectiveness of the methodological elaborated guide.

ÍNDICE

Introducción

Inmersa en la Era de la Información[1], que desde el punto de vista económico significa la capacidad de capitalizar las tecnologías actuales y el crecimiento de las infraestructuras existentes; Cuba ha potenciado el desarrollo de aplicaciones capaces de soportar las infraestructuras y ha diseñado los flujos informativos como salidas de nuevos productos y servicios, con la implementación de herramientas capaces de manipular los contenidos informacionales sobre un amplio sistema de redes.

Dentro de la organizaciones todo el volumen informacional se procesa soportado en las tecnologías informáticas y de las comunicaciones (en lo adelante TICs), factor que permite un aumento del volumen de información por lo que se hace cada vez más urgente la protección de esa información generada y la determinación de su flujo dentro en cada una de las entidades, para que sea útil a todo el personal que la necesite.[2]

Para ello Cuba a partir del año 2007 elaboró un Reglamento para el uso de estas Tecnologías, el cual vio la luz a partir de Agosto del 2007 en la Resolución 127 del Ministro de Informática y las Comunicaciones, respaldado por el acuerdo 6058. Reglamento que establece los procedimientos a seguir para proteger las propiedades esenciales de la información, los cuales luego de un adecuado análisis de riesgo, deben ser reflejados en el plan de seguridad informática de cada entidad.

En marzo del 2011 la Contraloría General de la República de Cuba (en lo adelante CGR) emite la Resolución 60, la cual dispone en su norma Actividades de Control que: El control de las TIC en las entidades se deberá integrar y conciliar con el Plan de Seguridad Informática y con su Sistema de Control Interno, en el que se definen las actividades de control apropiadas a partir de la importancia de los bienes e información a proteger, en correspondencia con la legislación vigente, considerando los riesgos y los permisos de acceso a los diferentes niveles de información automatizada y refiere además que para diseñar el Sistema de Control Interno se deberá garantizar la seguridad de la información que se genere adoptando las medidas que permitan la integridad, confidencialidad, oportunidad y disponibilidad de datos y recursos.

Desde finales del siglo pasado, el control de los activos informacionales, ha estado adquiriendo

[1] Usualmente se utilizan los términos de Sociedad de la Información y Informatización de la Sociedad, cuando las formaciones socio-económicas realmente no han cambiado sino las formas y portadores. Por lo que realmente debe hablarse de Era de la Información. En cuanto a la Informatización de la Sociedad, realmente debe referirse a la Socialización de la Informática. Véase “Retos y Tendencias” en Ciencia, Innovación y Desarrollo, Vol. 5, No. 2, 2000.

[2] Sophos. (27 de Mayo de 2008). CUCERT. Recuperado el 3 de Diciembre de 2009, de http://www.cucert.co.cu/lectu.php

mayor importancia en los diferentes países, a causa de los numerosos problemas que ha ocasionado la ineficacia del mismo.

El aumento constante del uso de la informática, al igual que la actualización continua de los elementos que componen la tecnología de este campo, obligan a los directivos a disponer de controles, políticas y procedimientos que aseguren la correcta utilización de los activos que la componen.

En la VI Comprobación Nacional al Control Interno se presentaron algunas dificultades con la revisión de las tecnologías. De forma general en el análisis de los resultados obtenidos en las comprobaciones nacionales al Control Interno y en encuestas realizadas a los auditores del sistema en la provincia de Cienfuegos, se pudo determinar que persisten dificultades reales a la hora de evaluar la eficiencia y operatividad de los sistemas informáticos implementados en las organizaciones objeto de control y persiste el descontrol de los activos informáticos, constituyendo esta una **situación problémica** real que se necesita erradicar.

A partir de estas premisas, la autora de este trabajo, responsable máxima de su concepción y ejecución en la organización base de la investigación, consideró la necesidad de enfocar científicamente la tarea encomendada e identificó el siguiente **problema científico:** Cómo perfeccionar la evaluación del control interno relacionado con los sistemas informáticos en las acciones de control que ejercen los auditores del Sistema de Auditoría en la provincia de Cienfuegos.

Se determinaron a partir de este estudio las prioridades de este tema y las orientaciones recibidas por la institución nacional para poder desarrollar sobre bases científicas la investigación, sustentada en la base real de determinación de necesidades.

Es por ello que la investigación sustenta la **hipótesis** de que el diseño de una guía metodológica facilitará la preparación de los auditores del Sistema de Auditoría para la evaluación del control interno relacionado con los sistemas informáticos.

Para cumplimentar y sustentar el tema de la investigación, la autora establece como **objetivo general:** Elaborar una guía metodológica que permita verificar el cumplimiento de lo establecido referente a los recursos de las tecnologías de la información y sus servicios asociados mejorando el sistema evaluación del control interno de los sistemas informáticos.

Objetivos específicos

- Realizar un estudio teórico de las cuestiones relacionadas con el Control Interno y la

Seguridad de las tecnologías de la Información.

- Identificar los temas que constituyen incumplimientos en la revisión del Sistema de Control Interno en el subsistema de auditoría, relacionados con las Tecnologías de la Información.
- Diseñar una guía metodológica que permita mejorar el sistema de evaluación del control interno existente en las entidades objeto de control, relacionado con la actividad y los sistemas informáticos.
- Validar la guía a través del criterio de expertos.

Variables de la investigación

Independiente: Guía metodológica - Dependiente: Control Interno

Esta investigación se sustentó en un enfoque integral de los métodos de investigación científica, ya que se emplean métodos, procedimientos y técnicas del nivel teórico, empíricos y matemáticos para la obtención, procesamiento y el análisis de los resultados, entre ellos el análisis de documentos, histórico-lógico, encuesta, observación participativa, síntesis, abstracción, concreción, inducción, medición, criterio de expertos y estadísticos.

Por la importancia que reviste el tema y su actualidad al perfeccionar el sistema de evaluación y control de las tecnologías de la información, de aportar a la organización una herramienta que permita transmitir confianza razonable respecto de la efectividad y eficiencia de las operaciones de control de las Tecnologías de la Información, la confiabilidad e integridad de la información, la protección de los activos informáticos y el cumplimiento de leyes y regulaciones establecidas sobre esta temática; la investigación realizará un ***aporte práctico***, pues no se encamina a la creación de una nueva teoría, sino a la solución de problemas reales.

Utilidad metodológica

Aportar nuevos métodos de trabajo para el control de los activos de información y en consecuencia del control interno, por lo que puede considerarse como un sistema de valor añadido en la gestión de las tecnologías de la información de cualquier entidad.

Propósito

El propósito de la investigación es diseñar una guía metodológica que permita mejorar el sistema de evaluación del control interno existente, relacionado con la actividad informática, en las órganos, organismos y entidades, sujetas a las acciones de control realizadas por la Contraloría General, y por el Sistema Nacional de Auditoría, lo que se puede hacer extensivo a las Unidades Centrales de Auditoría Interna, Unidades de Auditoría Interna y Auditores Internos de los diferentes Organismos y

Organizaciones de la Administración Central del Estado, al realizar la evaluación de cada uno de los componentes del Control Interno desde la perspectiva del control de las tecnologías de la información y relacionar cada uno de los componentes que lo integran con las actividades propias de la organización.

Diseño.

La investigación se asume como explicativa - descriptiva, para poder cumplir con el objetivo central, y detalla la esencia de la problemática detectada, determinando las necesidades reales de la Contraloría para determinar los puntos a incluir en la guía metodológica.

Muestreo.

El universo poblacional de esta investigación son todos los auditores del Sistema. La muestra seleccionada para esta investigación fueron los auditores de la Contraloría Provincial de Cienfuegos.

El informe muestra en un primer capitulo algunos conceptos y temas sobre Control Interno y la Seguridad de las TICs, en un segundo capitulo presenta la propuesta de la Guía, y el tercer capítulo muestra la validación y aplicación de la guía.

CAPÍTULO I

El control es simultáneo, pero no presupone interferencias.
Raúl Castro Ruz, Enero 2012

Control Interno. Generalidades y proyecciones.

1.1 Aspectos generales sobre el Control Interno.

El control interno ha sido diseñado, aplicado y considerado a lo largo de su historia como la herramienta más importante para el logro de los objetivos, la utilización eficiente de los recursos y para obtener la productividad, además de prevenir fraudes, errores, violación a principios y normas contable, fiscal y tributaria.

Hasta la fecha, la expresión "control interno" carece de una definición apropiada o universal, o que sea aceptada o aprobada por todos los que investigaron el tema. No existe una completa unificación del significado de la expresión y se utilizan con frecuencia denotando lo mismo, los vocablos internal check e internal control, mientras que en idioma castellano se usan expresiones tales como: "control interno" (la más amplia o utilizada), "comprobaciones interior" o "comprobación interna y control"[3].
Las instituciones realizan grandes esfuerzos planificando, desarrollando e implantando nuevas y mejores formas de hacer negocios para aumentar así su productividad. Se invierten recursos en el mercadeo de productos y servicios, en tecnología, capacitación en áreas operativas y en la mejora del servicio al cliente. Sin embargo, muchas veces no le otorga la debida importancia al Control Interno que debe estar vigente en cada uno de los eslabones del sistema productivo de la institución.
Dentro de una organización el proceso administrativo constituye un desarrollo armónico donde están presentes las funciones de Planeación – Organización – Dirección y Control. El control en su concepción más general examina con anterioridad determinada realidad que aprueba o corrige. Es el proceso de determinar lo que se está llevando a cabo, a fin de establecer las medidas correctivas necesarias y así evitar desviaciones en la ejecución de los planes. Puesto que el control implica la existencia de metas y planes, generalmente mientras más claros, completos y coordinados sean los mismos y más largo el período que ellos comprenden; más completo podrá ser el control, sin embargo el mejor control previene que sucedan las desviaciones, anticipándose a ellas.

[3] Calderín, L. M. (2 de febrero de 2005). B*ibliociencias.* Recuperado el 2010 de abril de 5, de http://www.bibliociencias.cu/gsdl/collect/revistas/index/assoc/HASH6e54/32a 38a83.dir/doc.pdf

Se acepta que “El control interno es el sistema interior de una compañía que está integrado por el plan de organización, la asignación de deberes y responsabilidades, el diseño de cuentas e informes y todas las medidas y métodos empleados 1) para proteger los activos; 2) obtener la exactitud de la contabilidad y de otros datos e informes operativos; 3) promover y juzgar la eficiencia de las operaciones de todos los aspectos de las actividades de la compañía, y 4) comunicar las políticas administrativas, y estimular el cumplimiento de las mismas. … Incluye mucho más que el sistema contable y cubre cosas como las prácticas de empleo y entrenamiento, control de calidad, planeación de la producción, políticas de ventas y auditoría interna”[4].

Es aceptado que el control interno se divida en dos categorías: controles administrativos y contables. Los primeros son procedimientos y métodos que se relacionan sobre todo con las operaciones de una empresa y con las directivas, políticas e informes administrativos. Incluyen el llamado plan de organización, los procedimientos y registros que se relacionan con los procesos de decisión que conducen a la autorización de operaciones por la administración. Los segundos consisten en los métodos, los procedimientos y el plan de organización, que se refieren sobre todo a la protección de los activos y a asegurar que las cuentas y los informes financieros sean confiables[5].

Un asunto importante para el efectivo desempeño estratégico y operacional de una organización es mantener una buena capacidad de maniobra ante el entorno y con los clientes, evitar desviaciones no deseadas, manejar información fiable y asegurar cumplimientos indispensables, limitando o neutralizando fuentes de riesgos. Todo esto hoy concierne al control interno[6].

Puede conceptuarse además, al Sistema de Control Interno como el conjunto de elementos, normas y procedimientos destinados a lograr, a través de una efectiva planificación, ejecución y control, el ejercicio eficiente de la gestión para el logro de los fines de la organización[7].

El sistema de control interno.

En la Ley No. 107 ¨De la Contraloría General de República de Cuba¨ se define como:

Sistema de Control Interno: A las acciones establecidas por la legislación especial en esta materia, que se diseñan y ejecutan por la administración, para asegurar la consecución de los objetivos siguientes:

4 Winkle, C. y. (1996). . “Auditoría”. Es válido referir que el ejemplar que se utilizó para esta cita fue impreso sin referencia a los nombres de los autores, la editorial, la fecha de edición y el número de edición.

5 Idem.

6 Carballosa Rodríguez, D. (2010). *Adecuación de la guía de auto-control interno al sector de la salud en la provincia de Cienfuegos.* Cienfuegos: Universidad "Carlos Rafael Rodríguez".

7 Idem

- ✓ Proteger y conservar el patrimonio contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilícito.
- ✓ Asegurar confiabilidad y oportunidad en la información que se recibe o se brinda.
- ✓ Garantizar la eficiencia y eficacia de las operaciones económicas, mercantiles u otras similares que se realicen, de acuerdo con su objeto social o encargo estatal.
- ✓ Cumplir con el ordenamiento jurídico.
- ✓ Cumplir con el ordenamiento técnico establecido por los organismos rectores, para el empleo de herramientas, equipos, instrumentos y otros medios de carácter similar, en la realización de los distintos procesos a su cargo[8].

Para diseñar, implementar, perfeccionar y verificar la efectividad del Sistema de Control Interno implementado en cada órgano, organismo, organización, entidad nacional y consejo de la administración, así como en las dependencias subordinadas, conforme a sus características, competencias y atribuciones, la máxima autoridad a su nivel y los demás dirigentes, además de los deberes establecidos en la legislación correspondiente, tienen los siguientes deberes:[9]

- ✓ Diseñar y proponer la estructura organizativa en correspondencia con su objeto social o las funciones estatales objeto de su competencia.
- ✓ Conocer, adecuar, aplicar, controlar y exigir el cumplimiento de las disposiciones legales emitidas por los organismos rectores y las específicas inherentes a su actividad
- ✓ Establecer las normas técnicas y regulaciones propias para el desarrollo del trabajo.
- ✓ Definir los procesos, subprocesos y actividades en cada unidad organizativa.
- ✓ Velar porque las funciones y atribuciones de los jefes a cada nivel estén aprobadas.
- ✓ Determinar, conforme a los calificadores de cargo aprobados, los deberes funcionales y la responsabilidad de cada trabajador.
- ✓ Elaborar los procedimientos para cumplir con los procesos definidos, determinar las funciones de los puestos de trabajo, las contrapartidas de cada operación y de la unidad organizativa, fijando la responsabilidad individual en correspondencia con los compromisos contraídos al acceder al cargo.

---

[8] Contraloría General de la República. (2009). *Ley 107.* La Habana: Ministerio de Justicia.

[9] Contraloría General de la República. (2009). *Ley 107 Capítulo X, Sección Primera, Artículo 79.* La Habana: Ministerio de Justicia.

.

- ✓ Mantener actualizados los manuales de organización, procedimientos, contabilidad y costo, según proceda.
- ✓ Identificar los riesgos asociados, puntos vulnerables y objetivos de control.
- ✓ Establecer sistemas que garanticen la confiabilidad y oportunidad de la información.
- ✓ Implementar mecanismos de prevención, control y monitoreo del Sistema de Control Interno para su perfeccionamiento continuo.
- ✓ Evaluar la eficacia del Sistema de Control Interno en el órgano colegiado de dirección y adoptar las medidas que procedan.
- ✓ Delegar atribuciones con carácter restrictivo a favor de autoridad mediante resolución debidamente fundamentada, detallando las actividades a desarrollar, el período y la forma en que se efectúa su control, sin que ello exonere de la responsabilidad asignada a la autoridad que delega.
- ✓ Difundir la observancia de valores éticos y morales, así como el cumplimiento del código de ética, reglamento disciplinario o de conducta que constituya un sólido fundamento moral para su conducción.
- ✓ Evaluar la conducta de dirigentes y demás trabajadores, orientando su integridad, compromiso personal y sentido de pertenencia a su entidad.
- ✓ Las demás que se determinen por el Contralor General para el cumplimiento del objetivo y misión fundamental de la Contraloría General de la República.

La máxima autoridad a su nivel, al detectar violaciones e irregularidades que afecten su Sistema de Control Interno, aplica las medidas administrativas que correspondan para su corrección y perfeccionamiento, así como impone las medidas disciplinarias a los responsables directos y colaterales en correspondencia con la gravedad de los hechos detectados, atendiendo al impacto económico y social. En los casos que resulten procedentes, denuncia a las autoridades correspondientes el presunto hecho delictivo, de conformidad con lo establecido en la legislación penal vigente[10].

Las máximas autoridades de los órganos, organismos, organizaciones, entidades nacionales y de los Consejos de la Administración Provincial del Poder Popular y del municipio especial Isla de la Juventud, informan inmediatamente ante la detección de ilegalidades a la Contraloría General de la República para el examen de los casos y modos operar que muestren interrelación, y las acciones

[10] Contraloría General de la República. (2009). *Ley 107 Capítulo X, Sección Primera, Artículo 81.* La Habana: Ministerio de Justicia.

para su rectificación y divulgación con fines preventivos[11].

La implantación de las medidas de control interno y la realización sistemática de los controles y de la aplicación de divisiones para erradicar las deficiencias detectadas, deben ser tareas priorizadas de cada dirigente y de todos los trabajadores, que redundarán en un incremento de la eficiencia económica y en la calidad y el resultado positivo de las actividades desarrolladas por cada entidad.

Un adecuado sistema de control interno comienza por la definición clara y sin cuestionamiento alguno ***de la responsabilidad de diseñarlo y mantenerlo, para que produzca información confiable y oportuna. Esa responsabilidad pertenece a la administración de la entidad***[12]***.***

Este existe por el interés de la propia administración. Así, el control interno es una herramienta útil mediante la cual la administración logra asegurar, tanto como sea razonable, la conducción ordenada y eficiente de las actividades de la empresa. El nivel de control debe partir de un análisis costo – beneficio.

La expresión control interno es interpretada o utilizada para enunciar las directrices emanadas de los dueños, propietarios o ejecutivos para dirigir, controlar y coordinar a sus subordinados dentro de la pirámide de la organización, sea esta de tipo lineal, mixta o funcional.[13]

Por mucho tiempo, el alcance del Sistema de Control Interno estuvo limitado a las áreas económicas, de manera que se hablaba al respecto como de un asunto inherente a las actividades de contabilidad y finanzas; por ende, las restantes áreas operacionales y, de hecho, sus trabajadores, no se sentían involucrados.[14]

La implantación de sistemas de Control Interno por sí sola, no garantiza el alcance de los objetivos propuestos en los mismos. Hace falta conciencia y comprometer al personal en la observancia y cumplimiento de las políticas, normas, procedimientos y disposiciones generales que involucra el Control Interno. La experiencia ha demostrado que cuando el personal, (empezando por los Directivos y Gerentes) no está consciente del rol que le corresponde llevar dentro de la estructura de Control Interno de la institución, los objetivos de control no son alcanzados. Por ello, es necesario que paralelamente al sistema de Control Interno se desarrolle en el personal, la conciencia de control.

En Cuba, donde la casi totalidad de las entidades y sus recursos son propiedad social,

---

[11] Idem

[12] Winkle, C. y. (1996). . “Auditoría”. Obra citada.

[13] Idem

[14] Capote, G. C. (2001). Recuperado el 12 de Abril de 2010, de http://www.dict.uh.cu/Revistas/economia_desarrollo/2001n-2/GabrielCapote.pdf

administrados por las instituciones estatales, la aplicación consecuente de sistemas de control interno en todos sus aspectos es vital. Por otra parte, quien pretenda obtener resultados de eficiencia, eficacia y economía en la gestión de su organización, no puede ignorar la planeación y aplicación de un Sistema de Control Interno con los requerimientos necesarios para lograr dichos objetivos.

Es conveniente observar en el diccionario las definiciones de las palabras control y controlar. Asimismo, es de suma importancia interpretar y asumir cada una de las definiciones particulares donde se encuentran todos los elementos necesarios para aplicar el control desde cualquier posición de dirección o administración.

Control: Comprobación, inspección, examen, crítica, dominio, supremacía.

Controlar: Comprobar, inspeccionar, examinar, revisar, tener bajo su dominio, dirigir y dominar[15].

Al analizar el control deben tenerse en cuenta sus elementos integrantes:

• *Establecimiento de estándares:* Es decir la aplicación de una unidad de medida, que servirá como modelo, guía o patrón sobre la base de lo cual se efectuará el control.

• *Medición de resultados*: La acción de medir la ejecución y los resultados, puede de algún modo modificar la misma unidad de medida.

• *Corrección*: La utilidad correcta y tangible del control está en la acción correctiva para integrar las desviaciones en relación con los estándares.

• *Retroalimentación*: Es el establecimiento de medidas correctivas da lugar a este proceso; es aquí donde se encuentra la relación más estrecha entre la planeación y el control.

Control significa mucho más que control financiero o contable, el control es una función básica dentro de cualquier proceso de organización y administración, que facilita la evaluación ejecutiva, incluyendo su seguimiento y revisión sistemática, ya que lo que no se controla no es posible que pueda ser dirigido eficientemente.

Entre los avances introducidos respecto al contenido y aplicación de sistemas de control interno es significativa su extensión más allá de lo solamente contable y también la orientación de que quede plasmado en el conjunto de manuales de organización, funciones, procesos y procedimientos que ha de establecer la entidad como parte de la institucionalización del sistema. Estas acciones aportan consistencia en la instrumentación del control interno[16].

---

[15] Microsoft Encarta® 2009.

[16] Calderín, L. M. (2 de febrero de 2005). *bibliociencias.* Recuperado el 2010 de abril de 5, de http://www.bibliociencias.cu/gsdl/collect/revistas/index/assoc/HASH6e54/32a 38a83.dir/doc.pdf

Los principios y métodos que rigen el diseño de los sistemas de control interno, se han consolidado por milenios de actividad contable y de auditoría[17]. Han evolucionado desde la época preliteraria hasta la actual era de la información y el conocimiento. En cada época, se han adaptado a las tecnologías imperantes de procesamiento de la información[18]. La actual etapa de desarrollo humano, caracterizada por la revolución informática y de las comunicaciones, no es una excepción. Sin embargo, en esta época los cambios han sido tantos y tan sustanciales, desde la introducción de la partida doble, en el Renacimiento, y del libro impreso en papel; que muchos contadores y auditores han sido rebasados, superados por esta marea incontenible que es la **informatización**.

1.2. El control interno de las Tecnologías de la Información.

La información constituye el principal y más valioso de los activos que posee una organización moderna. De ahí que como tendencia se impone la introducción de sistemas automatizados para el procesamiento de los grandes lotes de transacciones generadas en los procesos de la gestión económico financiera de una entidad, sin embargo, el uso de estas nuevas formas de procesamiento trae aparejado nuevos riesgos para la exactitud, confiabilidad, custodia e integridad de los datos procesados, de ahí que sea necesario revisar los mecanismos de control interno que hasta este momento se aplican a los procesos contables tradicionales (manuales) y evaluar nuevas formas que involucren a los procesos informáticos y las tecnologías que los soportan.

El control interno es una de las piedras angulares en las que históricamente han confiado las entidades para la protección de sus activos. Los contadores, auditores y sistematizadores crearon y desarrollaron sus principios a través de milenios de contabilidad, durante los diferentes estadios de evolución de la sociedad humana. En los primeros años de este nuevo siglo, la informatización invade todas las actividades humanas, entre ellas, por supuesto, las contables, económicas y financieras. Ello crea la necesidad de que los principios básicos de control interno evolucionen también y se pongan en consonancia con las nuevas realidades[19].

La introducción de los sistemas informatizados no ha cambiado en nada el espíritu de esos planteamientos, al menos en lo referido a lo referido a las consideraciones contables, económicas y financieras; aunque el reconocimiento de que la información, el conocimiento y el capital humano en general, son algunos de los activos más importantes de una entidad, ha ampliado bastante su

[17] Hay quiénes erróneamente piensan que la contabilidad nació en la Italia renacentista con Paccioli y otros adelantados que lo precedieron y sucedieron. Nada más equivocado: hubo contabilidad (de partida simple) y auditoría desde milenios antes, en la China imperial, en el Egipto faraónico y en mucho otros lugares y épocas. La contabilidad y la auditoría precedieron, incluso, a la propia escritura. Desde ese entonces ambas han estado evolucionando.

[18] Lázaro, B. E. (2001). El control interno en los sistemas informáticos de las pequeñas y medianas empresas. La Habana, Cuba: Universidad de La Habana.

[19] Idem.

campo de acción[20].

Pero sí ha cambiado la forma en que se debe implementar y aplicar el control interno. Sí ha cambiado la manera en que se debe concebir las medidas y acciones de control interno. No olvidar que un sistema informatizado contable no es un sistema manual (formado solamente por seres humanos) ni automático (integrado totalmente por máquinas): es un sistema hombre-máquina, con todas las implicaciones filosóficas y prácticas que esto tiene. Es ahí donde está la verdadera diferencia entre la era pre-informática y la era informática y de las comunicaciones. Es ahí donde se debe centrar la atención, donde se exigirá despojarse de prejuicios y de criterios preconcebidos y consolidados en la mente humana por siglos de aplicación de métodos, criterios y estilos de trabajo condicionados por la utilización de formas de procesamiento de la información ya superadas.

Se deberá analizar entonces algunos de los principales cambios que se introducen con el procesamiento automatizado de la información y su repercusión en el control interno.

Ø ***Falta de registros y evidencias visibles***. En los sistemas manuales es observable el procesamiento completo de la información y sus controles a nivel de cada transacción generada, a través de documentos, sin embargo, en los sistemas automatizados todo o buena parte de este procesamiento, controles y resultados, quedan atrapados dentro de los procedimientos programados, no siendo visibles para el usuario, independientemente que los resultados finales se impriman y certifiquen (submayores, comprobantes de operaciones, mayor detallado).

Ø ***Disminución de la cantidad de personas involucradas en el procesamiento de datos***. Al automatizar cualquier actividad disminuye el número de participantes, pues las tecnologías suplantan el trabajo humano, por lo que a veces la falta de controles adecuados, puede conspirar contra la segregación de funciones, pudiendo alterarse datos o procesos impunemente.

Ø ***Diversos grados de dependencia del personal informático***. Antes de la introducción de la informática cada área y especialista era capaz de satisfacer el procesamiento de su información por si solo, sin embargo después de introducirse la informática, los mecanismos de control interno podrán ser debilitados, por falta de conocimientos sobre las aplicaciones que explota, dominio de técnicas relacionados con la informática, ante eventuales interrupciones de los sistemas y redes datos, etcétera, que solo son resueltas por personal especializado en la actividad.

Ø ***Almacenamiento de grandes volúmenes de datos en soportes magnéticos***. A diferencia de archivos de documentos sobre papel, los ficheros sobre soportes magnéticos pueden alterarse sin dejar rastros en procesamientos no autorizados, o simplemente destruidos por errores, delitos o

[20] Idem.

accidentes si no existen los controles adecuados.

Ø ***Acceso a los datos desde terminales o computadoras remotas***. Cuando se trabaja con redes de datos internas o conectadas mediante redes externas (INTERNET) puede peligrar la integridad de la información por la presencia de intrusos o virus informáticos.

Ø ***Transacciones generadas internamente***. Muchos sistemas automatizados generan transacciones internamente, sin que sean originadas por la entrada de datos, como por ejemplo el cálculo de la nómina de un sueldista cuando no existen incidencias en el mes, o que generen extensos procesamientos con solo el cambio de fecha, como puede ser el cierre de las operaciones del año, lo cual resulta de sumo interés para establecer políticas de control interno[21].

Para la evaluación de un adecuado sistema de control interno que involucre a los procesos informáticos debemos tener en cuenta cuales son los principales requerimientos que todo proceso informático debe cumplir. Para ello definamos dos variables:

Proceso informático fiable: Es aquel que se realiza en condiciones seguras y correctas de hardware, programas eficaces e instrucciones de operaciones ejecutadas correctamente.

Información fiable: Es aquella cuyos datos cumplen la condición de ser completos, exactos, oportunos, autorizados y provienen de un proceso informático fiable.

Bajo estas condiciones de fiabilidad tanto del proceso como de la información que se va a procesar entonces podemos evaluar el control interno atendiendo a los siguientes principios:

1. **Consistencia del procesamiento**: A diferencia del procesamiento manual que está influido por errores humanos, las operaciones que se ejecutan en computadoras serán siempre las mismas a iguales condiciones de programas, datos e instrucciones de operación despreciando prácticamente los errores de hardware. En esto reside lo consistente del procesamiento automatizado que lo hace ventajoso en grado extremo al procesamiento manual.

2. **Oportunidad y continuidad del procesamiento**: Toda entidad dependiente de sistemas de procesamiento automatizados deberá garantizar la oportunidad y continuidad del proceso, para lo cual se establecen planes de contingencia que permitan continuar procesando la información en lugares y computadoras alternativas.

3. **Completitud de los datos**: En todos los sistemas se programan controles que permiten igualar o mejorar la fiabilidad que alcanzan sistemas manuales, de que todos los datos que correspondan sean procesados, para ello se establecen procedimientos programados de control de secuencias, balanceo de totales de control, etcétera.

[21] Pino, R. G. (2009). El control interno y los sistemas automatizados para la Gestión Económica. La Habana, Cuba.

4. **Oportunidad de los datos**: A través de controles programados (controles de fecha) se puede lograr mayor fiabilidad de que los datos capturados y procesados se correspondan con el período considerado que en sistemas manuales.

5. **Exactitud de datos y procesamiento**: Uno de los puntos de mayor riesgo en el proceso informático lo constituye la entrada de datos, y posteriormente los mecanismos de detección de datos errados, su control hasta y durante la corrección hasta que sean devueltos para su reinserción dentro del sistema. Para lograr mayor exactitud y minimizar el riesgo de entradas de datos erróneos, se debe lograr en el diseño de los sistemas informáticos, la entrada, de una sola vez, de un dato que pueda ser usado en diferentes módulos de una misma aplicación. Para establecer una mayor exactitud durante la entrada de datos, se establecen controles programados, comúnmente llamados validaciones de entrada de datos, que pueden ser chequeos contra ficheros maestros, dígitos de chequeo, chequeo de fechas ilógicas, etc. También deberán establecerse controles para verificar la fiabilidad del proceso, como son controles de limite, datos no blancos, datos con signo contrario, etcétera.

6. **Autorización de datos y procesamiento**. Todos los datos que se procesan en los sistemas informáticos deberán estar correctamente autorizados de acuerdo a los niveles de accesos que sean programados así como también determinados procesos como son cierre de operaciones, confirmación de documentos, etc., deberán ser ejecutados con cierto nivel de autorización.

Teniendo en cuenta el amplio espectro que abarcan los controles dentro de un sistema de gestión automatizado se pueden clasificarlos dentro de dos grandes grupos: *Controles Generales y Controles Específicos o de Aplicaciones*.

Los *Controles Generales* son aquellos que van dirigidos a minimizar el impacto que puede tener el procesamiento electrónico sobre los sistemas informáticos, mientras que por otra parte los controles de aplicación están relacionados con tareas específicas que se ejecutan durante el procesamiento de los datos por ejemplo: accesos, captación de los datos, salidas impresas, etcétera.

Veamos a continuación que aspectos conforman estos dos grupos de controles:

- Controles Generales: Este grupo incluye la siguiente clasificación.

- Controles de Organización: Estos controles están vinculados fundamentalmente con las funciones que desempeñan los usuarios, diseñadores, programadores, etc. de las aplicaciones, así como con la responsabilidad por el control que tienen cada uno de estos sujetos que participan dentro del proceso de la gestión de la información. Estos controles juegan un rol esencial, pues evitan la concentración de funciones en una sola persona, o sea la autorización, ejecución, registro de transacciones y mantenimiento de las aplicaciones deben estar separadas.

- Controles de Hardware y Software: Estos controles aseguran calidad y seguridad ante fallas técnicas que presenta el equipamiento (computadoras, equipamiento de redes, impresoras, etc.), así como el control que se tienen sobre los mantenimientos periódicos de estos medios, de manera que se puedan asegurar con determinado grado de confiabilidad que funcionen los sistemas operativos, utilitarios, compiladores, aplicaciones, etc. Estos últimos también serán objeto de controles que aseguren la protección de los datos que procesan.

- Controles de Seguridad de las Aplicaciones: Incluyen aquellos controles encaminados a proveer de determinado grado de seguridad a los sistemas mediante la detección de fallas por distintos factores así como la recuperación ante dicha falla.

Los controles generales vinculados con las aplicaciones usualmente son interdependientes, pues en ocasiones su operación es esencial para la eficacia de los controles de aplicación, ya que la finalidad de los generales es establecer un marco general sobre las actividades del sistema de información, y brindar un nivel de seguridad aceptable para que se logren los objetivos de control interno.

Controles de Aplicaciones

El conocimiento y puesta en práctica de una política adecuada de los controles de aplicaciones constituyen un requisito esencial dentro de la evaluación de los riesgos a que pueden estar sometidos los sistemas de gestión contable por lo que le prestaremos especial atención dentro de este trabajo.

Estos controles se clasifican en:

1. **Controles de Accesos**: Todos los sistemas de información automatizados deberán incluir controles para su seguridad diseñados sobre la base del uso de palabras claves (password) y el uso de trazas de auditoría, que permita, bajo cualquier circunstancia, verificar que transacciones fueran ejecutadas y quién fue el usuario que la ejecutó.

2. **Controles de Entrada**: La violación de estos controles ponen en riesgo toda la información que será procesada, pues es mediante la adecuada implementación de estos que se asegura por ejemplo que la información se corresponda con el período en cuestión, que esté correctamente clasificada, que no exista duplicidad, que transacciones procedentes de otras fuentes también automatizadas no hayan sido modificadas, etc. Estos tipos de controles pueden ser tipificados como *preventivos*, que aseguren que la entrada de datos sea confiable y válida, los *detectivos* que identifican datos erróneos o no confiables y los *correctivos* que aseguran la realización de enmiendas en los datos errados antes de ser procesados.

3. **Controles de procesamiento**: El procesamiento como función interna de una computadora, es la

que asegura que todos los procedimientos programados en la aplicación se ejecuten de manera exacta y sin interrupciones, por ejemplo comparaciones de saldos, totalizar los importes de un documento, cálculo de un salario, etc. De ahí que sea extremadamente importante el establecimiento de controles que detecten y corrijan errores durante el procesamiento, que pueden estar en cálculos erróneos, utilización de programas no actualizados, uso de datos contenidos en ficheros alterados, etc.

4. **Controles de Salidas**: Las salidas de datos después del procesamiento podrán ser mostradas sobre diferentes soportes: impreso en papel, en pantalla o en soportes legibles (CD, disquetes, etc). La implementación de estos controles está encaminada a disminuir los riesgos en la información que será divulgada en cuanto a que sea recibida por usuarios no autorizados, que la información no es la adecuada o está incompleta o indebidamente clasificada. Las violaciones de estos controles puede provocar destrucción de datos por personas no autorizadas, comisión de delitos al manipular salidas relacionadas con cheques, facturas, etc, que sean analizados datos sobre la situación financiera que son errados.

Un adecuado análisis y la posterior elaboración de estrategias de control, teniendo en cuenta la clasificación anterior por parte de todas las personas involucrados en los procesos de automatización, permitirá garantizar que la gestión contable que se procese de esta forma, sea confiable, segura, oportuna y consistente.

Como médula fundamental del Control Interno que permite documentar las directivas referentes a la seguridad de los sistemas informáticos está el *Plan de Seguridad Informática* y contra *Contingencias*, el cual es responsabilidad de todas las personas involucradas de cualquier forma dentro de la explotación de las tecnologías informáticas.

Para lograr la efectividad de un Plan de Seguridad Informática se deberá incluir:

- Un plan de seguridad referente a la privacidad y a la seguridad informática tendente a garantizar que el sistema cuente con medidas de seguridad apropiadas y a un costo razonable.
- Reglas y objetivos de seguridad específicos para cada aplicación en cuestión.
- Una administración que abarque todas las etapas del ciclo de vida de los sistemas, haciendo énfasis sobre las medidas de seguridad a tomar frente a las modificaciones que se realizan sobre la aplicación.
- Un responsable de la aplicación que comprende con profundidad los objetivos, tecnologías y entorno de procesamiento.
- Un Plan contra Contingencias es de vital importancia para garantizar la continuidad del procesamiento de la información en condiciones anómalas eventuales y ante la ocurrencia de

desastres. En función de los requerimientos más importantes para evitar la paralización de los procesos se debe asegurar:

· Fuente de Energía ininterrumpida. (UPS).

· Verificación de los circuitos de forma periódica.

· Ubicación de los equipos en lugares seguros.

· Copias de programas y bases de datos almacenadas en lugares seguros.

1.2.1. El Control Interno y los riesgos inherentes al ambiente de sistemas de información automatizados.

El desarrollo de la informatización ha conllevado a que el procesamiento de los datos primarios contables se haya incrementado sobre la base del uso de tecnologías de la información, por lo que ha sido necesario tomar las medidas pertinentes que aseguren un nivel razonable de seguridad en cuanto al uso de la informática y la contabilidad y se requiere del auditor la aplicación de enfoques de Control Interno adaptados a estas nuevas exigencias.

El auditor interno tendrá en cuenta en su desempeño hacia los sistemas informáticos, lo establecido en la Resolución 340/2004 del Ministerio de Finanzas y precios que pone en vigor los procedimientos para los sistemas contables-financieros soportados sobre las tecnologías de la información y establece la obligatoriedad de que estos cuenten con la certificación otorgada por la entidad ministerial que se asigna al efecto, previo dictamen de una comisión integrada por especialistas de ambos ministerios, sobre la seguridad y protección del sistema y el grado de adaptación a las Normas Contables Cubanas.

Además el auditor debe conocer y tener en cuenta que los riesgos en los sistemas informáticos pueden provenir de:

- Deficiencias en actividades generales del sistema de información automatizado.
- Desarrollo y mantenimiento de programas.
- Soporte tecnológico de los softwares de sistemas.
- Operaciones.
- Seguridad física.
- Control sobre el acceso a programas.

Los riesgos pueden incrementar el potencial de errores o irregularidades en aplicaciones puntuales, en bases de datos, en archivos maestros o en actividades de procesamiento específicos.

La naturaleza de los riesgos y las características del Control Interno integrado al sistema de información automatizado incluye lo siguiente:

- Falta de rastro de las transacciones.

.Algunos sistemas de información automatizados son diseñados de modo que un rastreo completo de una transacción que podría ser útil para fines de la Auditoría Interna, existe sólo por un corto período de tiempo o únicamente en forma legible por computadora.

Un sistema complejo de aplicaciones incluye un gran número de procedimientos que pueden no dejar un rastro completo, por consiguiente, los errores en la lógica de un programa de aplicaciones pueden ser difíciles de detectar oportunamente por procedimientos manuales.

- Falta de segregación de funciones.

Algunos procedimientos de control que normalmente son desempeñados por el personal a través de sistemas manuales en forma individual, pueden ser concentrados en un sistema de información automatizado. Se debe tener en cuenta que un mismo trabajador no debe tener acceso a los programas automatizados, al procesamiento de la información y a los datos que se obtienen a través de la computadora, porque el desempeño simultáneo de estas funciones es incompatible.

Todos estos elementos deberán ser tenidos en consideración, pero se deberá conocer además la base legal que rige y controla todo lo referido a los ambientes informatizados.

1.3. Base legal para el Control de las Tecnologías de la Información.

En Cuba a partir del año 2007 se decide realizar un reordenamiento del uso de las Tecnologías de la Información y las Comunicaciones por lo que el Consejo de Estado y de Ministros de la República decide en su acuerdo 6058 fechado el 9 de Julio del 2007 aprobar los lineamientos para el perfeccionamiento de la Seguridad de las Tecnologías de la Información en el país, otorgando facultad legal al Ministerio de Informática y las comunicaciones para establecer las regulaciones correspondientes, así como las normas para la prestación de servicios de seguridad informática a terceros.

A partir del otorgamiento de esta facultad surge la Resolución 127/07 del citado ministerio donde se establece el Reglamento de Seguridad para las Tecnologías de la Información, el cual se estructura en siete (7) capítulos, los cuales incluyen 100 artículos que deben cumplir todas las personas naturales y jurídicas radicadas del territorio nacional.

A partir de las nuevas concepciones de la economía mundial y de los profundos cambios que ha asumido Cuba, la CGR emite la Resolución 60/11, fechada el 1 de Marzo del 2011. La referida Resolución establece en su segundo POR CUANTO: La necesidad de continuar perfeccionando el control interno, aconsejan dejar sin efectos legales las Resoluciones No. 297, de 23 de septiembre de 2003, dictada por la Ministra de Finanzas y Precios y No. 13, de 18 de enero de 2006, dictada

por la Ministra de Auditoría y Control, y emitir una nueva norma atemperada a las disposiciones que regulan esta actividad y a los requerimientos del desarrollo económico-administrativo del país[22].

A raíz del surgimiento de la citada Resolución 60 se establecen requerimientos específicos para el control de la TICS, y refiere en el Componente **Actividades de Control**, sección tercera, inciso e): En el control de las tecnologías de la información y las comunicaciones que los órganos, organismos, organizaciones y demás entidades que cuenten con tecnologías de la información y las comunicaciones, integran y concilian el Plan de Seguridad Informática con su Sistema de Control Interno, en el que se definen las actividades de control apropiadas a partir de la importancia de los bienes e información a proteger, en correspondencia con la legislación vigente, considerando los riesgos a que están sometidos; los permisos de acceso a los diferentes niveles de información automatizada, que deben quedar registrados mediante el documento que corresponda, debidamente firmado[23].

En su capítulo III, establece en su sección primera. DE LOS CONTROLES GENERALES. ARTÍCULO 15. Los órganos, organismos, organizaciones y demás entidades que poseen tecnologías de la información y las comunicaciones para el diseño e implementación del Sistema de Control Interno, garantizan la seguridad de la información durante el proceso, intercambio, reproducción y conservación de la misma, adoptando las medidas que permitan la integridad, confidencialidad, oportunidad y disponibilidad de datos y recursos, mediante la aplicación efectiva de los controles generales de las tecnologías de la información y las comunicaciones: controles de seguridad lógica, de seguridad física, de adquisición y desarrollo de programas, de garantía de la continuidad del proceso de información, de organización, entre otros.

Sección segunda. DE LOS CONTROLES A LOS SISTEMAS DE APLICACIÓN. ARTÍCULO 16. Los controles a los sistemas de aplicación soportados sobre las tecnologías de la información y las comunicaciones, garantizan la seguridad del procesamiento de las transacciones u operaciones, incluyen los procedimientos manuales asociados, requiriéndose una efectiva combinación con los controles generales para asegurar el cumplimiento de los requisitos de la información en correspondencia con los principios básicos del Sistema de Control Interno[24].

Sección tercera

DE LA CERTIFICACIÓN DE LOS SISTEMAS CONTABLE – FINANCIEROS SOPORTADOS SOBRE LAS TECNOLOGÍAS DE LA INFORMACIÓN

[22] Contraloría General de la República. (Marzo de 2011). Resolución 60. La Habana, Habana, Cuba.

[23] Idem

[24] Idem

ARTÍCULO 17. Los órganos, organismos, organizaciones y demás entidades para mantener de forma razonable la efectividad del Sistema de Control Interno, están obligados a utilizar sistemas contable – financieros, certificados por los ministerios de Finanzas y Precios y de la Informática y las Comunicaciones, de forma tal que se garantice la seguridad y protección de los sistemas automatizados expuestos en el Plan de Seguridad Informática.

1.4. La auditoría y el Control Interno.

En el desarrollo de los procedimientos de auditoría, ayuda a los auditores la forma organizada en que los sistemas de Contabilidad registran, clasifican y resumen los datos. El flujo de los datos contables empieza con el registro de las transacciones que se realizan diariamente en una empresa[25].

Los auditores pueden seguir la corriente de evidencias retrocediendo hasta sus orígenes. Este proceso del trabajo marchando hacia atrás desde las cifras de los estados hasta la evidencia detallada de las transacciones individuales es lo opuesto del proceso contable.

Aun cuando los procesos específicos de la auditoría varían de un trabajo a otro, los pasos fundamentales en que se sustenta el proceso de auditoría son esencialmente los mismos en casi todos los trabajos. Estos pasos fundamentales son:

1. Revisar y preparar una descripción escrita del sistema de control interno del cliente.
2. Probar la operación del sistema de control interno para saber si se cumple la descripción escrita.
3. Evaluar la efectividad del sistema de control interno.
4. Prepara un informe para la administración que contenga recomendaciones para mejorar el sistema de control interno.
5. Completar la auditoría: llevar a cabo pruebas para comprobar y justificar los saldos específicos de los saldos de las cuentas, y llevar a cabo otros procedimientos de auditoria.
6. Emitir el dictamen de auditoria.

La secuencia de estos pasos proporciona un marco lógico para el proceso de auditoría. Los auditores no necesitan sin embargo completar cada una de estas tareas antes de pasar a la siguiente; pueden emprenderse varias etapas del proceso al mismo tiempo. Por supuesto, el dictamen de auditoría, no puede emitirse hasta que se termina todo el trabajo de auditoria.

Revisión del Control Interno.

La naturaleza y lo extenso del trabajo de auditoria por llevar a cabo en un trabajo en particular

[25] Calderín, L. M. (2 de febrero de 2005). *bibliociencias.* Recuperado el 2010 de abril de 5, de http://www.bibliociencias.cu/gsdl/collect/revistas/index/assoc/HASH6e54/32a 38a83.dir/doc.pdf

depende principalmente de la efectividad del sistema de control interno del cliente para evitar errores de importancia. Antes de que los auditores puedan evaluar la efectividad del sistema necesitan tener conocimiento y comprensión de cómo trabaja: que procedimientos se siguen y quienes lo ejecutan, qué controles funcionan, como se procesan y registran las diferentes tipos de transacciones, y que registros contables y documentación de apoyo existen. Por lo tanto, una revisión del sistema de control interno es el primer paso lógico en cada trabajo de auditoria.

Las fuentes de información a cerca del sistema, incluyen las entrevistas con el personal, los papeles de trabajo de las auditorías de años anteriores y los manuales de procedimientos. Al reunir información acerca de un sistema, es útil a menudo estudiar la secuencia de procedimientos que se usa en el procesamiento de transacciones de las categorías principales.

En el transcurso de la auditoría se requiere un conocimiento práctico del sistema; en consecuencia los auditores deberán prepara un papel de trabajo que describa plenamente su comprensión del sistema. La descripción de este se prepara generalmente en forma de narración escrita, de gráficos de flujo, o como un cuestionario.

1.5. La auditoría de las Tecnologías Informáticas y su relación con el control.

Las informaciones soportadas en las TI, pueden ser accedidas de forma irregular (fraude) por personas de la propia organización y personas externas a la organización. Pudiendo generar así la pérdida de estos activos intangibles. Lo anterior lleva al entendimiento que este volumen informacional que se genera debe estar respaldado por el diseño de un sistema que asegure la seguridad de las propiedades esenciales de esta información: integridad, disponibilidad y confidencialidad.

Para combatir este tipo de crimen la auditoria en sistemas informatizados podrá tener un papel de suma importancia, utilizándose técnicas de auditoria y técnicas de desenvolvimiento de sistemas informatizados, para el control y para la identificación[26].

En diversas literaturas aparece reflejado indistintamente el término de sistemas informatizados y sistemas de información, en esta investigación la autora se referirá esencialmente a los sistemas de información, acotando que el término "*sistema de información*" se utiliza generalmente para denominar el procesamiento de datos generados internamente, relativos a las transacciones (tales como compras y ventas), y a las actividades operativas internas (tal como proceso de producción). De esta manera los sistemas de información pueden ser informatizados, manuales o bien una mezcla de los dos.

[26] Arima, C. I. (2002). Auditoría contras fraudes de sistemas informatizados. Brasil.

Los Sistemas de Información de las empresas están formados por los programas, aplicaciones, datos, recursos físicos y el personal que los utiliza, por lo que en la actualidad, la misión de ellos, en una empresa, es facilitar la consecución de sus objetivos estratégicos y para ello, se invierte una considerable cantidad de recursos en personal, sistemas y tecnología, además de los costos derivados de la posible organización estructural que muchas veces conlleva la introducción de estas tecnologías.

Esta importante inversión debe ser constantemente justificada en términos de eficacia y eficiencia materializadas por el estudio de las principales debilidades del sistema informático: hardware - software – datos - usuarios.

Los tres primeros puntos conforman el llamado **Triángulo de Debilidades del Sistema**:

Ø ***Hardware***: es la parte física, pueden producirse errores intermitentes, conexiones sueltas, sustracción o cambio del medio, etc.

Ø ***Software***: puede producirse la sustracción de programas, ejecución errónea, modificación, defectos en llamadas al sistema, etc.

Ø ***Datos***: puede producirse la alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.

Estas debilidades están dadas por el uso incorrecto intencional o no intencional del cuarto elemento mencionado: ***usuario***.

La Resolución 60/2011 de la CGR, define que el sistema de información está constituido por los métodos y procedimientos establecidos para registrar, procesar, resumir e informar sobre las operaciones de una entidad. La calidad de la información que brinda el sistema afecta la capacidad de los directivos y ejecutivos para adoptar decisiones adecuadas que permitan controlar las actividades de la entidad.

El sistema deberá contar con mecanismos de seguridad que alcancen a las entradas, procesos, almacenamiento y salidas. Sustentará la formulación y supervisión del Presupuesto de Ingresos y gastos en divisas, con información sobre los aspectos operacionales específicos y su comparación con las metas prefijadas. Toda esta información, en definitivas, pasará a constituir el antecedente para la rendición de la gestión.

El sistema de información debe ser controlado con el objetivo de garantizar su correcto funcionamiento y asegurar el control del proceso de los diversos tipos de transacciones.

La seguridad del sistema de información es la estructura de control para proteger la integridad, confidencialidad y disponibilidad de datos y recursos de tecnología de información.

La concepción general del término *seguridad*, puede entenderse por la facultad de estar cubierto de

algún riesgo o amenaza, pero si se hace una introspección a los sistemas y bienes informáticos se debe atraer a colación una serie de conceptualizaciones de carácter global para poder definir acertadamente el término de seguridad informática.

Estas conceptualizaciones son tomadas del anexo Principales términos y definiciones del Reglamento para las Tecnologías de la Información, emitido por el Ministerio de Informática y Comunicaciones, a raíz de lo dispuesto en el apartado segundo del Acuerdo 6058 suscrito el 9 de Julio del 2007 por el Comité Ejecutivo del Consejo de Estados y de Ministros de la República de Cuba.[27]

La seguridad informática está relacionada con la preservación de la confidencialidad, integridad y disponibilidad de la información tratada por los ordenadores y las redes de comunicación. Es la encargada de la identificación de las vulnerabilidades del sistema y del establecimiento de contramedidas que eviten que las distintas amenazas posibles exploten dichas vulnerabilidades.

Es determinante establecer acciones que propicien una protección de la información que logre satisfacer, lo más posible, las necesidades de información de los usuarios de una institución, por lo que los directivos deben proyectar la disposición de controles, políticas y procedimientos que aseguren la correcta utilización de los activos y recursos que la componen y por lo tanto, la auditoria a esta temática los provee de una herramienta que permite evaluar el estado de los controles establecidos[28].

Dentro de los ambientes informatizados se deberán ejecutar controles que permitan ponderar la objetividad y necesidad del uso de la informática para obtener la información. Por no tenerse esto muy en cuenta, han ocurrido incidentes informáticos relacionados con fuga de información, imprecisión en las salidas de información, unidos a un incorrecto uso y a una inadecuada manipulación, propiciando en muchos casos, no atender o dar por hecho que lo que se obtiene de la computadora es lo válido y lo correcto, obviando el análisis y el respaldo que esa información en ocasiones requiere.

Por lo cual se hace necesario vincular el significado del trabajo en un ambiente electrónico de datos con la fiabilidad y factibilidad de la información que este brinda y el empleo que se le debe dar a esa información por parte del personal que necesita acceder e ella.

El Che dijo al respecto, cuando todavía era incipiente el uso de las tecnologías para el procesamiento de datos: **“No se puede dirigir si no se sabe analizar y no se puede analizar si**

[27] Ministerio de Informática y las Comunicaciones. (2007). Acuerdo 6058. La Habana, Cuba.

[28] Fernández, T. R. (2009). Impacto de la Auditoría a las Tecnologías de la Información en la corporación Copextel S.A. La Habana, Cuba.

no existen datos verídicos", los cuales no existen si no se realiza un diseño de sistema que permita preservar la integridad, disponibilidad y confidencialidad de los datos que se procesen y si no se realizan y aplican controles al sistema y a las tecnologías que lo soportan.

Motivo por el cual, la ***Auditoría Informática***, como se le conoce desde sus inicios y más adelante como ***Auditoría a las Tecnologías de la Información*** adquiere gran importancia dentro de las organizaciones en el contexto actual.

En Cuba se introduce oficialmente el término de Auditoría Informática a partir del Acuerdo No. 4374, del 11 de abril del 2002 del Comité Ejecutivo del Consejo de Ministros[29], donde se define que la Auditoría de las Tecnologías de la Información consiste en:

- el examen de las políticas, procedimientos y utilización de los recursos informáticos;
- confiabilidad y validez de la información y,
- efectividad de los controles en las áreas, las aplicaciones, los sistemas de redes y otros vinculados a la actividad informática.

La auditoría informática crece en importancia a la par que la informática y los sistemas informáticos. Practicar auditorías en un ambiente computarizado, donde la informatización de los sistemas de gestión y contables han alcanzado un desarrollo tan notable, supone la introducción de una concepción muy diferente a la que primó durante décadas; con nuevos enfoques en los que inexcusablemente, la informática tiene que participar activamente como una valiosísima herramienta, que permita a esta disciplina evolucionar al mismo ritmo de las transformaciones incorporadas a la estructura del registro y el control interno.

La Resolución 350 del 2007 emitida por el extinto Ministerio de Auditoría y Control[30] al clasificar las Auditorías Internas en función de los objetivos que se persiguen en las mismas, identifica la Auditoría de Tecnología de la Información como, "el examen de las políticas, procedimientos y utilización de los recursos informáticos; confiabilidad y validez de la información, efectividad de los controles en las áreas, las aplicaciones, los sistemas de redes y otros vinculados a la actividad informática", reafirmando lo establecido en el Acuerdo No. 4374.

En el del Manual del Auditor[31], se expresa que: La Auditoría a las Tecnologías de la Información no cambia la función de la auditoría, ni tampoco la condición y cualidades de auditor. Un elemento clave para planificar una auditoría a las tecnologías de la información es traducir

[29] Comité Ejecutivo del Consejo de Ministros. (11 de abril de 2002). Acuerdo No. 4374. La Habana, Cuba.

[30] Ministerio de Auditoría y Control. (2007). Resolución 350. La Habana, Cuba.

[31] Ministerio de Auditoria y Control. (30 de agosto de 2002). Manual del auditor - Capítulo VII - Auditoría de las TICs. La Habana, Cuba.

los objetivos básicos a objetivos específicos; ellos pueden enmarcarse en los siguientes puntos:

Ø Que se cumplan las políticas, normas y procedimientos que rigen esta actividad.

Ø Que se compruebe la seguridad de los recursos (personales, datos, equipamiento y software).

Ø Que se garantice, que la información que se procese sea confiable.

Ø Que se verifique el grado de privacidad del ambiente informático.

En el citado manual se ofrecen indicaciones para la Auditoría a los Sistemas de Información, la cual deberá contemplar entre sus objetivos:

- Establecer los grados de calidad, seguridad, oportunidad y privacidad que presenta la información y satisfaga al usuario.
- Revisar la ubicación del departamento, del equipamiento y del personal de informática para verificar la segregación de funciones y la seguridad física de todos los componentes.

Y dentro de está se deberá evaluar el sistema de control interno de la entidad, verificando:

- Que los trabajos de planeamiento, desarrollo, operación y mantenimiento estén documentados y controlados.
- El aprovechamiento y rendimiento de los sistemas.
- Que se haya realizado un estudio de análisis de riesgos.
- Que los controles de seguridad estén establecidos tanto en los procesos manuales como automatizados.

Dentro de la Auditoría al ambiente informático, se tendrá en consideración, siguiente objetivo:

- Conocer el grado de confianza que la entidad puede tener en sus recursos informáticos, el nivel de seguridad, privacidad y confiabilidad que le ofrece el servicio informático al proceso de su Sistema de información.

Y dentro de está se deberá evaluar el sistema de control interno de la entidad, verificando:

- Que la automatización de los procesos de la entidad obedezca a políticas, normativas y procedimientos.
- Que exista un adecuado y eficiente plan de seguridad informática para el resguardo de los activos físicos y lógicos.
- Que se controle la consistencia, eficacia, economía, eficiencia y confiabilidad de los sistemas y aplicaciones en explotación.
- Que se asegure una adecuada y eficaz operación de los equipos y de los sistemas de información.

Pueden considerarse otras esferas o áreas relacionadas con la informática que pueden ser objeto de auditoría de Sistemas de Información y que al igual que las antes expuestas se sometan a las mismas etapas, pruebas y evaluaciones de control interno.

La auditoria de sistemas debe actuar en cualquier sistema de información de la empresa, sea a escala estratégica, sea a escala gerencial u operacional[32]. Para alcanzar los objetivos propuestos, los trabajos deben agrupar 4 líneas maestras de actuación:

Auditoria de sistemas en producción: sistemas ya implantados y en funcionamiento.

Auditoria durante el desenvolvimiento de sistemas: engloba la fase de construcción de sistemas de información.

Auditoria de ambiente de tecnología de información: engloba las estructuras orgánicas, contratos de hardware y software, normas técnicas y operacionales, costos, nivel de utilización de los equipamientos y el control adecuado de estos recursos, planes de seguridad y contingencia.

Auditoria de eventos específicos: engloba el análisis de causa, de consecuencia y de la acción correctiva posible, de eventos localizados y que no se encuentran bajo auditoria, detectados por otros órganos y llevados a su conocimiento (característica correctiva.

Entre los 4 tópicos de arriba, se puede afirmar que la auditoria en ambientes de tecnología de información es el más crítico. Los argumentos que la justifican son que las fallas encontradas en este punto son las que generan los problemas de (a), (b) y (d). Si no existe un control de ambiente interno donde la tecnología es utilizada, probablemente inexisten controles en los sistemas ya existentes, así como en los que serán desenvueltos y también es prácticamente nula la posibilidad de detectar fallas en eventos específicos.

La Ley 107 de la Contraloría General de la República, en su reglamento, sección tercera, define la ***auditoría de Tecnologías de la Información***: como el examen de las políticas, procedimientos y utilización de los recursos informáticos, así como la confiabilidad y validez de la información, la efectividad de los controles, aplicaciones, sistemas de redes, y otros vinculados a la actividad informática[33].

Dentro de la auditoría de Tecnologías de la Información se atenderá además del sistema de información al equipamiento que lo sustenta o sea al hardware.

En la auditoría al control del hardware y al software se utilizan diferentes técnicas o métodos

[32] Arima, C. I. (2002). Auditoría contras fraudes de sistemas informatizados. Brasil.

[33] Contraloría General de la República. (2009). *Ley 107 Capítulo IV, Sección Tercera, Artículo 43, inciso g).* La Habana: Ministerio de Justicia.

prácticos de investigación y prueba establecidas por el extinto Ministerio de Auditoría y Control, su aplicación, por los especialistas, está dada para lograr las evidencias, mediante revisiones necesarias que fundamentan los criterios del auditor.

Las técnicas más empleados son: Muestreo, Inspección, Observación, Confirmación, análisis, certificación, entre otras

En el Manual del Auditor, Capítulo: Muestreo y Otras Técnicas de Auditoría, se describen estas técnicas, en el presente trabajo la autora pretende dar una visión desde el punto de vista informático.

Muestreo: Teniendo en cuenta las diferencias entre los medios, es necesario la selección de las muestras por características, por ejemplo:

- Muestras por computadoras y monitores.
- Muestras por impresoras.
- Muestras por fuentes de alimentación.

Si esta selección no se realiza de esta manera se corre el riesgo de tomar una muestra muy amplia pero con las mismas características.

Inspección: Es el examen minucioso de los recursos físicos y documentos para determinar su existencia y autenticidad de un activo. Es imprescindible el trabajo con el control de los Activos Fijos Tangibles del área económica.

Observación: Presencia física del medio o su autorización para la no presencia.

Confirmación: Se utiliza para verificar que coincidan las configuraciones con el escaneo realizado durante la auditoría, la información que tiene el especialista de la actividad y la que tiene la Dirección de Sistemas de Información.

Análisis: Se analizan todos los documentos relacionados con el tema, involucra también la separación en diversa partes de una operación o de las distintas influencias sobre la misma.

Independiente, en la práctica, el auditor puede utilizar otras técnicas cuando el desarrollo de la auditoría lo requiera para la obtención de las evidencias necesarias.

La responsabilidad que tienen todos los usuarios de las tecnologías de la información (se incluye a los informáticos) sobre los medios que tienen bajo custodia no se limita a la firma del Acta de Responsabilidad o Acta de custodia sobre Bienes y Recursos Materiales, es un compromiso que se asume por la salvaguarda de la integridad física de los medios.

El progreso de la tecnología de la información, las limitaciones por parte de los usuarios para la adquisición de medios informáticos entre otras causas, trae consigo que el control de los recursos físicos informáticos sea uno de los objetivos principales de la Auditoria de las

Tecnologías Informáticas.

1.5.1 Pruebas de cumplimiento para evaluar los Controles Internos en la auditoria informática.

Al revisar y documentar controles en un ambiente computarizado, el auditor realiza investigaciones y pruebas de revisión, estudio y evaluación del sistema de contabilidad y los controles internos correspondientes vinculados a la auditoría. Los controles generales y los de aplicación pueden identificarse y documentarse mediante el uso de técnicas de diagramas de flujo, cuestionarios, etc.

La eficacia y la eficiencia de las pruebas de cumplimiento en un ambiente computarizado se pueden mejorar usando las técnicas de auditoría asistidas por computadoras. El uso de estas técnicas puede ser adecuado cuando el sistema no tiene evidencia visible que documente el rendimiento de los controles en que el auditor se va a apoyar. En este caso, los datos de pruebas se pueden usar para obtener evidencia, por ejemplo, de que los controles de acceso a la información en sistemas en línea están funcionando según se diseñaron.

Si el auditor obtiene evidencia de que los controles no estaban operando de acuerdo a la manera en que fueron diseñados, o si las pruebas de cumplimiento indican que los controles generales no fundamentan una seguridad de que los de aplicación funcionen durante el período que examina el auditor, puede dejarlos y tratar de alcanzar los objetivos de auditoría mediante la aplicación de pruebas sustantivas.

En cumplimiento de la LEY No.107 de la CGR y como parte del Plan Anual de Auditoría, se lleva a cabo la Comprobación Nacional al Control Interno, en estrecha coordinación con el Sistema Nacional de Auditoría y la ANEC, en el interés de dar continuidad al trabajo, en aras de fomentar una cultura de probidad y eficiente control económico-administrativo de las entidades, sobre la base del cumplimiento del orden, la disciplina y la legalidad.

Cada año, en el Programa de la Comprobación Nacional al Control Interno se plantea entre sus objetivos "Verificar cuestiones relacionadas con las tecnologías de la información"., específicamente en la VI Comprobación Nacional se debía verificar, lo siguiente:

1.- Si existe evidencia documental que acredite que el sistema contable financiero soportado en las TI, está certificado por el nivel que corresponde. Especificar por cada sistema informático utilizado, fecha de certificación y entidad que lo expide.

2.- Si hay evidencia documental de la aprobación por quien corresponda, de los usuarios con acceso a los sistemas contable financieros.

3.- Si los sistemas tienen protección mediante contraseña, si éstas no son visualizadas en la pantalla y si están definidos varios niveles de acceso.

Entre las principales deficiencias detectadas en las organizaciones, durante la VI Comprobación Nacional se pueden señalar:

- Acceso por personal no autorizado al software contable implementados.
- Carencia de evidencia documental para acceso al software contable.
- Software contables no certificados.
- Movimiento de activos informáticos no realizados.
- Descontrol de piezas y partes de los equipos informáticos.

En la actualidad la evaluación del sistema de control interno de las TICs se realiza a través de comprobaciones muy sencillas y no se hace de manera permanente una evaluación del estado del control interno a partir de las deficiencias detectadas durante el proceso de revisión.

Por lo que se hace necesario elaborar una guía que permita evaluar y controlar la eficiencia y eficacia de los Sistemas de informáticos implementados y todos los recursos con que cuenta la organización.

Conclusiones parciales

En este capítulo se explicitaron temas relacionados con el Control interno de las Tecnologías Informáticas y se detallaron los cambios surgidos a partir de la Resolución 60, la cual dedica su tercer capítulo al control de estos recursos, motivo por el cual se puede concluir que a partir de los cambios en la legislación vigente relacionada con los controles informáticos se hace necesario elaborar una guía que facilite el control y evaluación del sistema de control interno de las tecnologías.

CAPÍTULO II

La experiencia nos ha enseñado que aquello que no se controla con efectividad, no se cumple o se ejecuta superficialmente.
Raúl Castro Ruz, Enero 2012

Diseño de la guía metodológica para la evaluación del Sistema de Control Interno a las tecnologías de la información.

Las profundas transformaciones que introduce la Resolución 60/11 de la CGR detalladas extensamente en el capítulo 1 llevan a realizar una revisión de la situación actual que presenta el sistema de auditoría, muestra de la investigación para realizar a partir de este diagnóstico, una guía que permita evaluar eficientemente el control interno de las tecnologías informáticas que responda al modelo actual que necesita Cuba para responder al fenómeno de la corrupción y las ilegalidades, ampliamente debatido en varios escenarios.

2.1. Caracterización del escenario de acción.

En la provincia de Cienfuegos el sistema nacional de auditoria cuenta con un total de 270 auditores, distribuidos de la siguiente forma:

Organismo	Total auditores	Formación profesional
CGR	57	Lic. Economía - 22 Lic. Contabilidad y Fzas - 22 Lic. Derecho – 4 Lic. Educación Esp. Informática – 2 Ing. Informático 1 Lic. Filología – 1 Lic. Economía de la Industria – 3 Lic. Economía política – 1 Ing. Industrial – 1 T/M Economía – 1 T/M Contabilidad - 1
UCAI CAP	Plantilla 117 Real 72	Lic. Economía – 7 Lic. Economía de la Industria – 3 Master Contabilidad – 1 T/M Contabilidad – 14 T/M Economía – 6 Formación emergente – 34 T/M Estadísticas – 3

		T/M Finanzas – 2 T/M planificación - 1
BPA	15	Ing. Industrial – 1 Lic. Contabilidad y Fzas – 6 Lic. Economía – 6 T/M Finanzas – 1 T/M planificación - 1
BANDEC	20	Ing. Mecánico – 1 Lic. Contabilidad – 1 Lic. Contabilidad y Fzas. – 3 Lic. Control Econ. – 1 Lic. Economía – 2 Lic. Informática – 1 T/M Contabilidad – 8 T/M Finanzas - 3
AUDITA	9	Lic. Contabilidad y Fzas. – 5 Lic. Economía – 2 Lic. Economía de la Industria - 2
ONEI	5	Lic. Economía de la Industria – 1 Lic. Control Económico – 1 Lic. Economía – 1 Formac. Emergente - 2
CIMEX	8	Lic. Economía – 2 Lic. Informática – 1 Lic. Econ. y planific. – 2 Lic. Contabilidad – 1 Lic. Contab. y Fzas - 2
ANEC	12	Lic. Control Económico – 4 Lic. Economía de la Industria – 1 Lic. Economía – 2 Lic. Contabilidad – 1 T/M Contabilidad – 2 Formac. Emergente - 2
MES	2	Lic. Economía - 2
MINCEX	1	Lic. Econ. Industria - 1
MINTUR	5	Lic. Economía – 2 Lic. Contab. y Fzas – 2 T/M Contabilidad - 1
MINAZ	10	Ingeniero Agrónomo – 1 Lic. Contabilidad y Finanzas – 2 Lic. Control Económico – 1 Lic. Dirección de la Economía - 1 Lic. Economía – 1

		T/M Economía – 1 T/M Contabilidad- 1 Formac. Emergente - 2
MFP	26	Ingeniero Agroindustrial Azucarera – 1 Lic. Contabilidad – 1 Lic. Control Económico – 1 Lic. Economía – 12 Lic. Economía de la Industria – 2 Lic. Economía Finanzas y Crédito – 1 Lic. Contab. y Fzas - 1 Técnico Medio Contabilidad – 4 Formac. Emergente – 1 T/M Finanzas – 1 Lic. Español –Literatura - 1
MINCULT	3	Lic. Contab. y Fzas - 1 Lic. Economía – 1 Lic. Economía de la Industria - 1
MINAL	3	Lic. Contab. y Fzas - 1 Lic. Economía de la Industria - 2
MINBAS	21	Ingeniero Energético Nuclear – 1 Lic. Contabilidad y Finanzas- 4 Lic. En Economía – 3 Formac. Emergente – 6 Lic. Economía de la Industria - 1 Lic. Contabilidad – 5 T/M Economía -1
MICONS	11	Lic. Finanzas – 1 Lic. Economía de la Industria - 1 Formac. Emergente - 9
MINAGRI	34	Lic. Contabilidad y Finanzas – 2 Lic. Economía – 10 Lic. Economía de la Industria - 1 Ing. Agronómo – 3 Formac. Emergente – 15 Lic. Contabilidad – 1 T/M Contabilidad – 1 Lic. Educación Esp. CE - 1
MIC	3	Lic. Economía – 2

		T/M Contabilidad – 1
MINCIN	3	T/M Contabilidad – 3
SIME	6	Lic. Economía de la Industria - 1 Formac. Emergente – 5
MINSAP	2	Lic. Contabilidad y Finanzas – 2
INRH	1	Lic. Economía - 1
UJC	2	Formac. Emergente – 2
PCC	3	Lic. Contabilidad y Finanzas – 1 T/M Contabilidad- 1 Formac. Emergente - 1
CTC	2	T/M Planificación de la Economía – 1 Lic. Economía - 1
MINED	2	Formac. Emergente - 2
MITRANS	6	Formac. Emergente - 6
ASPORT	1	Lic. Contabilidad – 1
MINIL	1	T/M Economía - 1
GAE	4	Formac. Emergente - 4
ASTILLEROS FAR	1	Formac. Emergente - 1
CUBALSE	1	Formac. Emergente - 1
MINCEX	3	Se desconoce
MINFAR	3	Se desconoce
FISCALIA	1	Se desconoce
MININT	2	Se desconoce

Como se puede observar es muy heterogénea la formación del personal inscrito en el registro de auditores que pertenece al Sistema Nacional de auditoría en la provincia de Cienfuegos, esta característica de por si muy distintiva impide que los conocimientos en materia informática alcanzados en la formación de pregrado de estos profesionales, no favorezca el accionar sobre el control de los recursos informáticos.

A partir de estos referentes la autora de la investigación decidió aplicar un modelo de determinación de necesidades, el modelo aplicado se sustenta los presupuestos teóricos que caracterizan la regularidad de este proceso y las relaciones que se establecen entre las mismas. Relaciones que se

manifiestan a través de tres dimensiones que son:

• Determinación de necesidades sociales.

• Determinación de necesidades en el desempeño laboral.

• Determinación de necesidades individuales.

Sobre la base de estos elementos y contrastando (lo ideal con lo real) se determinan las necesidades de los auditores del sistema apoyados por la información recopilada a través de técnicas participativas como la entrevista grupal y la valoración de controles realizados a las tecnologías informáticas, esto unido a la revisión documental y el lógico proceso de análisis valorativo permitió establecer los aspectos que con mayor incidencia afectan el desempeño profesional en las acciones de control relacionadas con las tecnologías informáticas; es decir:

- Escaso dominio de la legislación vigente relacionada con la actividad.
- Falta de actualidad, expresada en el insuficiente dominio de las técnicas a aplicar en las acciones de control.
- Carencia manifiesta de habilidades para la integración de los conocimientos y su aplicación a la solución de problemas profesionales en este tipo de acciones de control.
- Insuficiente acciones de capacitación que permitan la actualización relacionada con estas temáticas.

2.2. Diagnóstico de la situación actual.

Se detalló ampliamente en el capítulo anterior la situación que presenta la evaluación del sistema de control interno de las tecnologías informáticas en las organizaciones del territorio, motivo por el cual se partirá de estos precedentes para desarrollar este epígrafe.

En la VI Comprobación Nacional al control interno desarrollada en el año 2011, se indicaba indagar por parte de los auditores los siguientes aspectos en el control de las tecnologías de la información:

1. Si existe evidencia documental que acredite que el sistema contable financiero soportado en las tecnologías de la información, está certificado por el nivel que corresponde. Especificar, por cada sistema informático utilizado, fecha de la certificación y entidad que expide.

2. Si hay evidencia documental de la aprobación por quien corresponda, de los usuarios con acceso a los sistemas contable-financieros.

3. Si los sistemas tienen protección mediante contraseñas, si éstas no son visualizadas en pantalla y si están definidos varios niveles de acceso[34].

En apariencia estos aspectos no tienen nada de complejo a la hora de realizar las comprobaciones, pero la realidad demostró otras aristas, cuando los auditores del sistema enfrentaron la tarea, no todas las organizaciones poseían sistemas que estuvieran certificados y cumplieran con estos requisitos por lo que a la hora de redactar y desarrollar el informe no sabían como describir la realidad objetiva encontrada en las organizaciones.

Se procedió a analizar la guía de autocontrol, emitida por la CGR, vigente al momento de desarrollarse la investigación, la cual reflejaba los siguientes aspectos:

No.	Aspectos a Verificar	SÍ	NO	NP
	COMPONENTE AMBIENTE DE CONTROL			
	Control del sistema de información			
1.	Existe un sistema de información con indicadores cuantitativos y cualitativos.			
2.	Existen procedimientos para las copias de seguridad, para la recuperación y la planeación de contingencia.			
3.	Existen controles sobre la adquisición, implementación y mantenimiento del software del Sistema.			
4.	Existen mecanismos de control que regulen la información que va dirigida a terceros.			
5.	Existen mecanismos de seguridad para las entradas, procesos, almacenamiento y salida de la información.			
6.	Se revisa y actualiza periódicamente los sistemas contable y presupuestario con el propósito de generar una garantía de exactitud de los registros.			
7.	Se han incorporado a los sistemas de información computarizados, cuando se requiere, la realización de conciliaciones, comparaciones y verificaciones en forma automática y la generación de reportes de inconsistencias.			
	Control de la tecnología de información			
8.	Existe un Plan de Seguridad Informática para proteger la integridad, confiabilidad y disponibilidad de datos y recursos de la tecnología de la información.			

[34] Estas indicaciones están recogidas en el manual de la VI Comprobación Nacional al Control Interno, específicamente para el Sector empresarial emitido por la Contraloría General de la República para tales fines.

No.	Aspectos a Verificar	SÍ	NO	NP
9.	Los sistemas contables-financieros tienen contraseñas y éstas no son visualizadas en pantalla.			
10.	Están establecidos los mecanismos para la implementación, supervisión y evaluación de los medios de computación.			
11.	La Información Clasificada se trabaja en microcomputadoras desconectadas de la Red.			
12.	Están establecidos los mecanismos para la utilización, implementación, supervisión y evaluación de la Información Clasificada.			

Realizando además un estudio de los antecedentes de las auditorías de las tecnologías de la información se pudo determinar que existen un total de 7 guías, por la cual se guían los auditores del sistema para realizar esta tipología de acciones:

Estas guías fueron confeccionadas por los distintos organismos de control que han existido en el país, entre los cuales se pueden referir, la Oficina Nacional de Auditoría (ONA) y el Ministerio de Auditoría de Control (MAC).

Las mismas en la etapa actual se encuentran fuera del contexto real, pues a raíz de los profundos cambios surgidos en el entorno nacional con la puesta en vigor del Reglamento para el uso de la Tecnologías de la Información sustentado en la Resolución No. 127/07 se hizo necesario perfeccionar aún más el control de los activos tangibles e intangibles soportados en estas tecnologías.

La Resolución 60 de la Contraloría General de la República del año 2011 (detallada en el epígrafe 1.4. del capítulo anterior) establece nuevas orientaciones para los sistemas de información soportados en las TI, pero además dedica un capítulo para el tratamiento del control de los activos informáticos.

La citada resolución establece además que para mayor control de estos activos, las organizaciones deben cotejar el plan de seguridad informática con el plan de prevención de riesgos.

Lo anteriormente descrito llevó a la autora de la investigación a determinar como objetivo general la elaboración de una guía metodológica que permita verificar el cumplimiento de lo establecido referente a los recursos de las tecnologías de la información y sus servicios asociados mejorando el sistema evaluación del control interno de la actividad informática.

Para dar cumplimiento a este objetivo se procedió a realizar un estudio de todas las guías

existentes, buscando puntos coincidentes que pudieran servir como referentes en el modelo propuesto y que estuvieran acordes a la legislación vigente, pudiendo determinar que:

Guía 1	Guía 2	Guía 3	Guía 4	Guía 5	Guía 6	Guía 7
Total aspectos 57	Total aspectos 13	Total aspectos 10	Total aspectos 39	Total aspectos 9	Total aspectos 15	Total aspectos 19
Coincidentes 14	Coincidentes 7	Coincidentes 8	Coincidentes 39	Coincidentes 7	Coincidentes 11	Coincidentes 8

Tabla 2.1

2.3. Elaboración de la guía metodológica para evaluar el sistema de control interno en las organizaciones.

Para la confección de la guía se tuvieron en consideración todos los referentes anteriores, y luego teniendo en consideración la legislación vigente en la materia y las necesidades cognitivas de los auditores del sistema, se procedió a la elaboración de la guía.

Esta guía se decidió confeccionar subdividiéndose por categorías, entre las que se pueden mencionar:

- Guía para auditar el Sistema de Seguridad Informática implementado en la entidad.
- Guía para auditar el proceso de mantenimiento de reparación de hardware.
- Guía para auditar el Plan de Seguridad Informática y de Contingencias.
- Guía para auditar aplicaciones contables y financieras.

GUÍA DE CONTROL PARA AUDITORIA DE SEGURIDAD INFORMÁTICA

Base legal: Resolución 127/2007 del MIC y Guía del CI de las TI según Res. 60/2011

No	Aspectos a Verificar	SÍ	NO	NP
	SISTEMA DE SEGURIDAD INFORMATICA			
1.	Se encuentra diseñado, implantado y actualizado un Sistema de Seguridad Informática. (Art.4 y 7)			
2.	Existen registros para dejar constancia escrita de las principales incidencias que ocurren, realización de las salvas de información, control de entrada y salida de bienes informáticos. (Art. 4)			
3.	Se analizan en los Consejos de Dirección u otros, temáticas sobre la seguridad de las tecnologías de la información y se deja constancia escrita en las actas (Acuerdo 6058 CECM inc. 4to)			
4.	Existe un Plan de Seguridad Informática para proteger la integridad, confiabilidad y disponibilidad de datos y recursos de la tecnología de la información. (Art. 6) (ver guía de revisión del plan de seguridad informática)			
5.	El PSI se encuentra firmado y aprobado por la máxima dirección de la entidad.			
6.	La entidad posee nombrado un especialista de Seguridad Informática y este conoce sus funciones. (Art.6 y 8)			

No	Aspectos a Verificar	SÍ	NO	NP
7.	Existe un adecuado conocimiento y conciencia de la Seguridad Informática por parte de la alta dirección de la organización como máxima responsable de la Seguridad Informática.			
8.	Está determinado el nivel de acceso de los usuarios a los bienes informáticos. (Art. 9a)			
9.	Existen políticas, normas y procedimientos escritos para la planificación, ejecución, evaluación y control del uso de las tecnologías de Información para el logro de los objetivos de la entidad.			
10.	Posee la entidad un plan de revisión y auditoria que determine los eventos y servicios que serán objeto de seguimiento.			
11.	Existen evidencias documentales sobre la realización de controles internos de seguridad informática que garanticen la supervisión sistemática sobre el empleo de las tecnologías y sus servicios. (Art. 9 inc d), 10 inc b), inc e) y 21)			
12.	Se imponen o proponen sanciones ante violaciones de seguridad. Art. 9f)			
13.	Se tienen definidas de forma explícita las violaciones de seguridad informática y las medidas disciplinarias que se adoptaran. (Art. 19) <u>Entre ellas:</u> • Uso no autorizado de las tecnologías informáticas y sus servicios. (Art. 21). • Realización de acciones no autorizadas de comprobaciones de vulnerabilidades contra sistemas informáticos nacionales o extranjeros. (Art. 25) • Introducir, ejecutar, distribuir o conservar en los medios informáticos programas que pueden ser utilizados para comprobar, monitorear o transgredir la seguridad; así como información contraria al interés social, la moral y las buenas costumbres. (Art. 26) • Realización de administración remota de los Servidores y estaciones de trabajo empleando conexiones conmutadas. (Art. 63) • Difundir a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas o que lesione la Seguridad Nacional. (Art. 79) • Vincular cuentas de correo electrónico de un Servidor de la entidad a Servidores en el exterior del país. (Art. 77) • Envío de mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (SPAM). (Art. 80) • Se accede sin autorización o se agrede a cualquier sistema de cómputo conectado a redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios. (Art. 85) • Explorar o monitorear las redes públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas. (Art. 84)			
14.	Se establecen controles que impiden la instalación de software y hardware sin la debida autorización. (Art. 10e, 43, 64)			
15.	Se prohíbe la introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones, sin que sean aprobados a partir de su correspondencia con el sistema de seguridad establecido y las necesidades de la entidad.			
	CLASIFICACIÓN Y CONTROL DE LOS BIENES			
16.	Los bienes informáticos de la entidad son utilizados en funciones de trabajo en correspondencia con su objeto social. (Art. 13)			
17.	Se posee un inventario de los bienes informáticos incluyendo sus componentes			

No	Aspectos a Verificar	SÍ	NO	NP
	y sus especificaciones técnicas y estos se encuentran incluidos en el expediente técnico de cada medio. (Art. 14)			
18.	Cada bien informático se encuentra bajo custodia documentada de una persona. (Acta de responsabilidad material) (Art. 15)			
19.	Se controla el movimiento de los medios informáticos. (Art.16, 41)			
20.	Se controlan los soportes de almacenamiento portátiles externos (memorias flash, laptop, cámaras fotográficas, discos duros, etc.) y de la información que almacenan. (Art. 16)			
	DEL PERSONAL			
21.	Se encuentra incluida como responsabilidad laboral del personal su responsabilidad en la seguridad informática. (Art. 17)			
22.	Se ha especificado al personal las medidas y procedimientos de seguridad establecidos en el Plan de Seguridad Informática. (Art. 9d)			
23.	Los contratos de empleo del personal especifican la vigencia de la responsabilidad del trabajador ante la seguridad informática aún cuando finalice su relación laboral. (Art. 19)			
24.	Posen los usuarios de Tecnologías Informáticas (TI) preparación necesaria sobre Seguridad Informática. (Art. 12a, 65)			
25.	La entidad ejecuta control del empleo de las TI. (Art. 22)			
26.	Existe conocimiento de los principales aspectos tratados en el plan de contingencia por parte del personal involucrado en las tareas de recuperación.			
	SEGURIDAD FISICA Y AMBIENTAL			
21.	Las TI que poseen información de valor están debidamente protegidas. (Art. 27, 29 a , 30, 31, 32, 33)			
22.	En las áreas controladas existe control de acceso para garantizar la entrada solo a personas autorizadas.			
23.	En estas áreas se controla la posibilidad de daño por fuego, inundaciones y otras formas de desastre natural o artificial.			
24.	El equipamiento instalado en las áreas controladas está protegido contra fallas de alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los procesos que deban continuar en caso de un fallo de electricidad prolongado, siendo ubicado y protegido de manera que reduzca los riesgos.			
25.	Se aplican medidas alternativas que permitan la protección de estos medios e impidan su empleo para cometer acciones malintencionadas.			
26.	Existen procedimientos escritos para garantizar que todas las tecnologías de información, independientemente de su importancia, estén protegidas contra alteraciones o sustracciones, ya sea de éstas o sus componentes, así como de la información que contienen. Se controla hasta nivel de componente			
27.	Se cumplen procedimientos para proteger la información contenida en equipos destinados a ser dados de baja u otras funciones.			
28.	Los dispositivos de almacenamiento que contengan información crítica para la entidad son destruido físicamente o sobrescritos completamente en lugar de borrarlos como usualmente se hace.			
29.	Los cables de alimentación o de comunicaciones que transporten datos o apoyen los servicios de información se protegen contra la intercepción o el daño.			
30.	Están separados y protegidos los cables de información (datos) de los de alimentación (voltaje). (Art. 37)			

31.	Se garantiza que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicio y especificaciones recomendados por el fabricante para asegurar su disponibilidad e integridad.			
32.	En caso de necesidad de envío de equipamiento fuera de las instalaciones para que reciban mantenimiento, se realizará en correspondencia con los procedimientos establecidos para ello, observando las regulaciones establecidas en el país en materia de protección a la información. (Art. 39 y 40)			
33.	Las TI están protegidas contra alteraciones, sustracciones, de estas o sus componentes (sellos de seguridad). (Art. 36)			
34.	Están planificadas las medidas de protección contra incendio.			
35.	Están conectadas las PC a fuentes de respaldo de energía con limitadores de voltaje.			
36.	Existe adecuado control de acceso a los locales donde se encuentran ubicadas las TI y están clasificadas las áreas donde se encuentran ubicados los servidores. (Art. 28-29)			
37.	Cuenta el local de ubicación de los servidores con adecuadas condiciones de seguridad. (Art. 29)			
38.	Se identifican de manera clara los parámetros de voltaje de las tomas de alimentación eléctrica.			
39.	Se realizan inspecciones sorpresivas para detectar las extracciones no autorizadas de bienes informáticos.			
	SEGURIDAD DE OPERACIONES			
40.	Al determinar las responsabilidades en las áreas informáticas se ha tenido en cuenta el principio de separación de funciones, considerando aquellas tareas que no deben ser realizadas por una misma persona, a fin de reducir oportunidades de modificación no autorizada o mal uso de los sistemas informáticos. (Art. 42)			
41.	Cuentan con procedimientos definidos que garantizan las acciones para cubrir las brechas de seguridad y la corrección de los errores del sistema de acuerdo a la legislación vigente: – solo el personal claramente identificado y autorizado tenga acceso a sistemas en funcionamiento y a los datos; – todas las acciones de emergencia tomadas sean documentadas detalladamente; – la acción de emergencia sea reportada a la dirección y realizada de manera ordenada. (Art. 44)			
42.	Se cumplen los procedimientos establecidos ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes. (Art. 51)			
	IDENTIFICACION, AUTENTICACION Y CONTROL DE ACCESO			
43.	En los sistemas en que es posible el acceso por múltiples usuarios se dispone para cada uno de ellos de un identificador de usuario personal y único; al que responden por las acciones que con ellos se realicen.			

44.	La asignación de identificadores de usuarios en los sistemas (sistemas operativos, sistemas de aplicación, páginas web, bases de datos, etc.), se realiza a partir de un procedimiento que incluye la notificación del jefe inmediato del usuario, solicitando el permiso de acceso y definiendo los derechos y privilegios. En caso de terminación de la necesidad del uso de los sistemas por el cese de la relación laboral u otras causas, se procede de forma análoga para la eliminación del identificador de usuario, o a la restricción de los niveles de acceso. (Art. 20, 45 y 46)			
45.	Se cumplen los requisitos definidos en la legislación vigente acerca de la asignación de contraseñas. – Serán privadas e intransferibles. – Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado para el acceso que protegen. – Combinarán en todos los casos letras y números sin un significado evidente, con una longitud mínima de 6 caracteres. – No pueden ser visualizadas en pantalla mientras se teclean. – No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información. (Art. 47)			
46.	Los sistemas de aplicación deben contar con: – La posibilidad de ser modificado y/o actualizado a versiones superiores, – la documentación y los ficheros fuentes; – Manuales de usuario y manuales de explotación. – Ayuda en línea para facilitar el trabajo de los usuarios.			
47.	Se encuentra implantado procedimiento escrito que otorga o suspende derecho de acceso a sistemas y datos para cada usuario. (Art. 48)			
48.	Se tiene elaborado un procedimiento o instrucción para autorizar y controlar el acceso a las tecnologías de información por personal ajeno a la entidad. (Art. 23)			
	SEGURIDAD ANTE PROGRAMAS MALIGNOS			
49.	Las TI se encuentran protegidas con programas antivirus. (Art. 50)			
50.	Tienen implementados los controles y procedimientos para protegerse contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para impedir su generalización (Art. 50)			
51.	Los antivirus utilizados están debidamente aprobados en el país y están actualizados. (Art. 50)			
	RESPALDO DE LA INFORMACION			
52.	Está implementado un sistema fiable de respaldo. (Art. 53)			
53.	Se dispone de dispositivos externos y equipos informáticos para la ejecución de copias de seguridad en la red. (Art. 53)			
54.	Los respaldos, con los informes de las copias y los procedimientos de recuperación son almacenados en otra ubicación diferente al origen. (Art. 54)			
55.	Los respaldos mantienen las mismas condiciones ambientales que el origen. (Art. 55)			
56.	Se realizan las salvas con la periodicidad definida y verifican su realización. (Art. 53 y 56)			
57.	Se prueban regularmente los respaldos de información para verificar su estado y uso ante emergencias. (Art. 56)			
58.	La información clasificada se trabaja en computadoras desconectadas de la red.			
59.	Existen mecanismos de control para la información que va dirigida a terceros.			
	SEGURIDAD EN REDES			
60.	Se encuentran implementados mecanismos de seguridad de redes. (Art. 57)			

61.	Si existe administración remota, esta se realiza de forma segura según lo indicado en las disposiciones vigentes. (Art. 63)			
62.	Existen procedimientos de verificación periódica de la seguridad de la red, para detectar posibles vulnerabilidades o se realizan pruebas de penetración o hackeos éticos contratados por entidades autorizadas para solucionar las vulnerabilidades.			
63.	La arquitectura y la configuración de los diferentes componentes de seguridad de una red y la implementación de sus servicios estarán en correspondencia con las políticas definidas y aprobadas para su empleo.			
64.	Se tiene un inventario actualizado de los dispositivos y medios existentes en el local de los Servidores. (Art. 10e)			
65.	Existe control de acceso al local de los servidores. (Art. 33, 34, 35)			
66.	Se tiene establecida una política de seguridad y medios de control para establecer los servicios autorizados, protocolos, puertos y reglas de accesos implementadas para garantizar que se bloqueen los no autorizados. (Art. 57)			
67.	Están habilitadas las opciones de seguridad con que cuentan los Sistemas Operativos que garantizan la protección de los servidores y terminales, el acceso a la información, el monitoreo y auditoria de los principales eventos por un tiempo no menor de 1 año. (Art. 58)			
68.	Los productos de fiscalización y monitoreo instalados son los autorizados en el país. (Art. 59)			
69.	La arquitectura y configuración de los componentes de seguridad de la red y la implementación de los servicios que presta, están en correspondencia con las políticas definidas y aprobadas para su empleo, no dejándose a la iniciativa de una persona. (Art. 60)			
70.	La red cuenta con un Administrador para su operación. (Art. 61)			
71.	Se prohíbe la adición de algún equipo o la introducción de cualquier tipo de software en una red, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la dirección de la entidad, garantizando su compatibilización con las medidas de seguridad establecidas para la protección de dicha red.			
72.	Se cumplen de acuerdo a la legislación vigente, las medidas necesarias para garantizar la integridad, confidencialidad y oportunidad de la información, de acuerdo a los servicios que recibe y oferta.			
73.	Cumple el administrador de red las obligaciones relacionadas con la Seguridad Informática según la legislación vigente. (Art. 62)			
74.	Se tiene prohibida la administración de redes mediante conexiones conmutadas de redes públicas. (Art. 63)			
75.	Están establecidas barreras de protección para conexiones desde o hacia el exterior de la entidad. (Art. 66)			
76.	Se tienen instrumentados y ejecutan procedimientos periódicos de verificación de seguridad de las redes que detecten posibles vulnerabilidades. (Art. 67)			
77.	Las informaciones colocadas en servidores para su acceso público tienen creados los procedimientos que garanticen integridad y disponibilidad en correspondencia con los intereses de la entidad y el país. (Art. 70)			
78.	Si un sitio se encuentra hospedado en un servidor en el extranjero, este es réplica o espejo del sitio principal del ubicado en Cuba, con medidas de seguridad durante su actualización. (Art. 71)			
79.	Se prohíbe colocar sitios o páginas Web desde entidades estatales en servidores en el extranjero que ofrecen estos servicios de forma gratuita. (Art. 72)			

80.	Los servidores destinados al uso de la red interna no contienen servidores destinados a facilitar accesos hacia o desde el exterior. (Art. 73)			
81.	La red corporativa que provee servicios internos los realiza por puertos identificados y con dispositivos de protección que garantizan el acceso a los servicios por personal autorizado. (Art.74)			
82.	Las conexiones externas de la red se utilizan en interés de la entidad. Las cuentas de estos usuarios están aprobadas por la dirección de la entidad. (Art. 75)			
83.	Está establecida la prohibición de habilitar cuentas de correos electrónicos desde la entidad en servidores que se encuentran en el exterior del país. Si existen están justificadas y autorizadas por la dirección, especificándose el tipo de información a transmitir y plazo de vigencia. (Art. 76)			
84.	Está establecida la prohibición de vincular cuentas de correo electrónico de un servidor de la entidad a un servidor en el exterior con el fin de redireccionarla y acceder a mensajes. (Art. 77)			
85.	Las listas de correos y los chat se encuentran autorizados en todos los casos por la dirección de la entidad. (Art. 78)			
86.	Está establecida la prohibición a través de la red, la transmisión de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas o lesione la seguridad nacional. Se cuenta con controles que lo detectan, informándose a las instancias pertinentes. (art. 79)			
87.	Se controla el envío de correos no solicitados a múltiples (spam) cualquier sea su carácter. (Art. 80)			
88.	Se toman las medidas requeridas para impedir la sobrecarga de los canales de comunicaciones, restringiendo el envío/recepción de gran volumen de información y generación de mensajes a múltiples destinatarios. (Art. 81)			
89.	Se tienen implementados controles dirigidos a impedir e interrumpir la generación de cadenas y el envío de mensajes de correos de forma masiva a través de la red. (Art. 82)			
90.	Los usuarios con conexiones remotas autorizadas conocen de sus obligaciones al usar este servicio. (Art. 83)			
91.	Está establecida la prohibición de exploración o monitoreo de redes públicas en busca de vulnerabilidades o información de usuarios. (Art. 84)			
	INCIDENTES DE SEGURIDAD			
92.	Tienen definida una estrategia ante incidentes o violaciones de la seguridad en correspondencia con la importancia de los bienes informáticos que posea y las alternativas a emplear. (Art. 86)			
93.	Existen medidas y procedimientos para llevar adelante la estrategia ante incidentes que garanticen continuidad, restablecimiento y recuperación de los procesos informáticos. (Art. 87)			
94.	Las medidas y procedimientos de recuperación responden a la identificación de eventos (riesgos) que causan interrupción o afectación de los procesos informáticos. Se incluyen los responsables de su cumplimiento y los recursos necesarios. (Art. 88)			
95.	Los procedimientos definidos para la gestión de incidentes o violación de la seguridad informática siguen los pasos establecidos para su correcta evaluación. (Art. 89)			
96.	Ante cualquier incidente que afecte la seguridad informática se tiene establecido crear la comisión para esclarecer los hechos y establecer las medidas que eviten recurrencia. (Art. 90)			

97.	Al producirse un incidente o violación, se reporta la información oportunamente a la OSRI y a la instancia superior de la entidad, de acuerdo a la importancia de la misma. (Art. 91)			
	PRESTACION DE SERVICOS A TERCEROS			
98.	En caso de prestar servicios informáticos a terceros se cuenta con la autorización emitida por la OSRI. (Art. 92)			
	INSPECCION A LA SEGURIDAD DE LAS TI			
99.	Se cumple que la inspección estatal en materia de seguridad a las TI es atribución del MIC, por lo cual la entidad no las realiza. (Art. 95)			
100.	El jefe de la entidad ha facultado bajo documento la realización de controles en materia de seguridad informática a las entidades subordinadas. (Art. 96)			
	TOTAL			

Nota:

- Deberá detallarse en hoja aparte, el por qué de aquellos aspectos declarados No Procede.
- Para calificar el resultado de esta guía, tomar el siguiente criterio:

Tomar como total los Si restándole los NP

Efectuar: C = (NO/SI) 100. Muy Bien ……. igual o mayor a 90 %

Bien ...entre 70 y 89 %

Regular …entre 60 y 69 %

Mal ...menor a 60 %

Otro criterio de evaluación puede tener en cuenta valorar el peso que tiene cada aspecto y no darle un tratamiento lineal como el considerado anteriormente, lo cual se ha asumido para facilitar el análisis.

A partir de esta guía general se decidió diseñar guías específicas que ayuden al auditor en el ejercicio de sus funciones y lo apoyen en aspectos medulares que le permitan ofrecer una valoración efectiva del control interno de las tecnologías.

GUÍA PARA AUDITAR EL PROCESO DE MANTENIMIENTO Y REPARACIÓN DE HARDWARE.

No	Aspectos a Verificar	SÍ	NO	NP
	INSPECCION A LOS MANTENIMIENTOS			
1.	Se controlan los materiales usados y entregados para la reparación de equipos de cómputo.			
2.	Existe contrato con terceros para la realización del mantenimiento planificado.			
3.	Se controla y describe el proceso de trabajo realizado en los expedientes de cada computadora.			
4.	Las órdenes de servicio reflejan la fecha de ejecución, el nombre y la firma del ejecutor.			
5.	Existe procedimiento escrito en el PSI relacionado con el destino final de las piezas y partes de los equipos de cómputo.			

- Revisar papel de trabajo que se anexa para la auditoría de hardware.

GUÍA PARA AUDITORIA DEL PLAN DE SEGURIDAD Y DE CONTINGENCIAS.

No	Aspectos a Verificar	SÍ	NO	NP
	REVISIÓN DEL PLAN DE SEGURIDAD INFORMÁTICA			
1.	Está conformado y actualizado el plan de seguridad informática en correspondencia con la legislación vigente.			
2.	El plan de Seguridad Informática se encuentra debidamente actualizado, firmado y aprobado por el director de la entidad.			
3.	El plan de Seguridad Informática se actualiza ante cambios de personal, locales, tecnologías, aplicaciones o servicios; la aparición de nuevas amenazas o la variación de la probabilidad de ocurrencia de alguna de las existentes			
4.	Existe la designación de él (los) responsable(s) de Seguridad Informática y preparación y conocimiento de los mismos para realizar sus funciones.			
5.	Se corresponden las políticas, controles y procedimientos plasmados en el PSI con la evaluación de riesgos realizada por la entidad.			
6.	Se corresponde la caracterización del entorno informático y la definición de los servicios con lo existente en la práctica.			
7.	En el Plan de Seguridad Informática aparecen determinadas las áreas o zonas controladas con requerimientos específicos, protegidas por un perímetro de seguridad definido en dependencia de la importancia de los bienes informáticos contenidos en ellas y su utilización de acuerdo a la legislación vigente.			
8.	El plan de Seguridad Informática contiene las políticas y procedimientos para la utilización, implementación, supervisión, evaluación y conservación de la Información Clasificada.			
9.	Se declaran y se cumplen adecuadamente los procedimientos establecidos en el Plan de Seguridad Informática para las copias de respaldo de la información contable.			
10.	Existen procedimientos escritos para garantizar la buena conservación de las copias de resguardo, durante su almacenamiento.			
11.	El plan de Seguridad Informática de la entidad contempla la protección contra programas malignos en todas las PC y los servicios principales de la Red como el correo, servicios de navegación por Internet y otros servicios susceptibles a los mismos.			
12.	Refleja el PSI procedimientos para la realización de auditorías internas a la seguridad de la información y las redes de datos donde se incluyen todos los servicios asociados.			
13.	Existe procedimiento declarado en el PSI relacionado con la introducción de cualquier tipo de software en una red, ya sea a través de soportes removibles o acceso a redes externas, sin la autorización de la dirección de la entidad.			
14.	Existe procedimiento declarado en el PSI relacionado con la asignación o el retiro de los identificadores de usuarios en los sistemas (SO, Sistemas de aplicación, páginas web, bases de datos,).			
15.	Se declaran en el PSI procedimientos para la restricción de los accesos a registros, datos y recursos.			
16.	Refleja el PSI procedimiento para las salvas de las trazas de los servicios de la red, especificando quién la realiza y con qué frecuencia.			
17.	Se recogen en el PSI los Registros establecidos en la entidad (Control de soporte y salvas, auditorias realizadas, Entrada Salida y movimiento de tecnología de información, Incidencias, trabajo en maquina, mantenimiento o reparación de roturas.) y el procedimiento para su empleo.			
18.	Existen registros para dejar constancia escrita de las principales incidencias que ocurren, realización de las salvas de información, control de entrada y salida de bienes informáticos.			
19.	Se tiene definido un procedimiento para regular y aprobar la introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones en correspondencia con el sistema de seguridad			
20.	Permiten los procedimientos del PSI proteger la integridad, confiabilidad y disponibilidad de datos y recursos de la tecnología de la información.			
	REVISIÓN DEL PLAN DE CONTINGENCIAS			
21.	¿Se ha elaborado un Plan de Contingencia para la Seguridad Informática?			

22.	Se basa el plan en un análisis muy cuidadoso del impacto de las perdidas de recursos de la organización e incluye todos los recursos del sistema (el equipamiento, software, datos, personal, y otras provisiones).			
23.	El Plan de Contingencia para la Seguridad Informática ha sido evaluado y aprobado por las instancias correspondientes.			
24.	Se encuentra actualizado a la realidad del contexto de aplicación.			
25.	En las áreas controladas existe control de acceso para garantizar la entrada solo a personas autorizadas y se controla la posibilidad de daño por fuego, inundaciones y otras formas de desastre natural o artificial.			
26.	Se encuentran definidos los procedimientos para la recuperación en caso de fallas de fluido eléctrico, fallas de hardware, Incendios, desastres naturales, hurtos, etc.			
27.	El plan precisa que el equipamiento instalado en las áreas controladas esté protegido contra fallas de alimentación y otras anomalías eléctricas, incluyendo el uso de fuentes de alimentación alternativas para los procesos que deban continuar en caso de un fallo de electricidad prolongado, siendo ubicado y protegido de manera que reduzca los riesgos.			
28.	Existe un conocimiento de los principales aspectos tratados en el Plan de Contingencia por parte del personal involucrado en las tareas de recuperación.			
29.	Las tareas de recuperación reflejadas en el plan son claras y están correctamente escritas quedando definida la responsabilidad por cada tarea enfocada a un individuo o departamento.			
30.	Cubre el plan la recuperación de todas las posibles fallas de seguridad del sistema, desde un error del operador hasta la posible total destrucción.			
31.	Se planifican pruebas de emergencia para determinar si el plan es realizable.			

GUÍA PARA AUDITORIA DE APLICACIONES CONTABLES Y FINANCIERAS.

No	Aspectos a Verificar	SÍ	NO	NP
	REVISIÓN DEL SISTEMA			
1.	Cuenta el sistema con: – La posibilidad de ser modificado y/o actualizado a versiones superiores, – la documentación y los ficheros fuentes; – Manuales de usuario y manuales de explotación.			
2.	Existe procedimiento escrito aprobado por la máxima dirección de la entidad que autorice el acceso de los usuarios al sistema contable y se definen en él los privilegios y tipos de acceso. (Anexo 1 Res. Conjunta MFP-MIC y 48 de la 127))			
3.	Se guardan y monitorean las trazas o registros de los principales eventos y operaciones que se ejecutan en el sistema.			
4.	El equipamiento que soporta el sistema contable financiero es utilizado solo por el personal autorizado.			
5.	Los usuarios que explotan el sistema han recibido las acciones de capacitación para mejorar su desempeño.			
6.	El sistema contable empleado por la entidad está certificado.			
7.	Dispone cada usuario de accede al sistema de un identificador único. (Art. 45 Res. 27)			
8.	Las salvas de la información del sistema se realizan en soportes externos y se guarda fuera del local donde se origina.			
9.	Existe un registro para el control de las salvas que se realizan donde se incluye nombre del personal que la realiza, fecha, hora.			

- Revisar procedimientos adjuntos para la auditoría a sistemas contables y financieros.(Anexo No. 4)

2.3.1. Características generales y novedosas de la guía.

La guía elaborada recoge todos los aspectos a considerar para el cumplimiento de la legislación vigente en las organizaciones, incluyendo en cada aspecto a revisar, el artículo de la resolución que lo establece o pone en vigor.

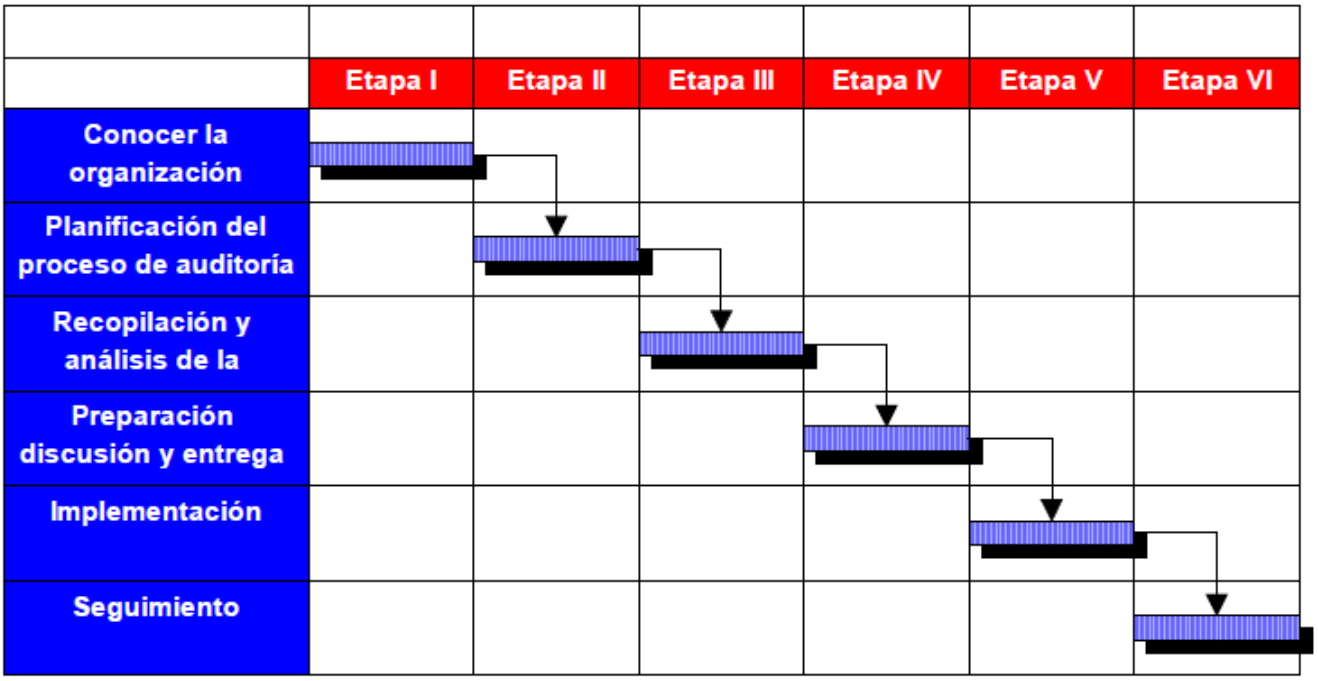
Se estructura de forma organizada y asequible partiendo del sistema de seguridad informática que es elemento de soporte de todo el flujo informacional de las organizaciones y de su estructura depende en gran medida el proceso de toma de decisiones para todas las acciones a acometer en el entorno organizacional.

Dentro de los aspectos inherentes al sistema se tienen en consideración los aspectos físicos y lógicos de las tecnologías que lo sustentan por lo cual se deberán revisar la seguridad física y ambiental de las tecnologías que sustentan la información.

La guía tiene en consideración que el factor más influyente dentro de un sistema informático es el factor humano, el cual deberá ser capacitado eficientemente para asumir la tarea de acceder al sistema informático implementado dentro de la organización.

2.4. Orientaciones metodológicas para la aplicación de la guía.

La guía se aplicará dentro del contexto de una auditoría a las TI, dicha tipología de auditoría quedó ampliamente debatida en el capítulo I, específicamente en el epígrafe 1.4, pero en este gráfico se recordarán las principales etapas por las que se deben transitar para lograr un control efectivo de la acciones de control emprendidas dentro de un entorno informático.



Luego de analizar estas etapas se recomienda aplicar la guía teniendo en consideración los siguientes elementos:

- El documento clave donde se describe las características del sistema informático implementado en las organizaciones, es el plan de seguridad informática, por lo que se recomienda empezar con la aplicación de la guía específica para auditar y revisar dicho plan, el cual generalmente siempre aparece unido al plan de recuperación ante contingencias.

- Luego de tener conocimiento de las características del sistema informático diseñado, el auditor deberá proceder a comprobar en el terreno las descripciones realizadas en dicho plan, para ver su correspondencia con la realidad objetiva implementada.

- Dentro de esta revisión el auditor podrá comprobar las características de las computadoras que se incluyen en el entorno para lo cual deberá partir de una muestra representativa, la cual deberá cotejar con el submayor de activos tangibles de la organización, se realizará un papel de trabajo contentivo de las descripciones físicas y las que realmente se encuentran en el submayor.

- Luego se procederá a revisar la existencia de los expedientes técnicos que cada una de las computadoras para cotejarlos con la evidencia real del entorno.

- Por último deberá proceder a la aplicación de la guía para la revisión de las aplicaciones contables y financieras.

Conclusiones parciales:

A partir de la estructuración que se le ofrece a la guía para evaluar el sistema de control interno de las tecnologías informáticas en las organizaciones se le ofrece a los auditores del sistema una herramienta que le facilitará su desempeño profesional.

CAPÍTULO III

Validación de la Guía metodológica para la evaluación del Sistema de Control Interno a las tecnologías de la información.

Este capítulo refleja la metodología empleada para efectuar el proceso de validación de los resultados de la investigación, los cuales muestran los resultados de los instrumentos y métodos empleados.

3.1 El método Delphi.

Para validar la guía metodológica diseñada se ha seleccionado el método del criterio de expertos, para lo cual la autora decide acotar que solicitó la concurrencia de personal calificado como especialista en temas informáticos.

Este método se aplicó con el objetivo de conocer las opiniones acerca de la guía, así como su pertinencia y viabilidad para la aplicación.

Para llegar a conformar consensos de opiniones en las investigaciones científicas se pueden emplear los llamados Métodos de grupos o métodos creativos de grupo, donde se utilizan métodos del tipo heurísticos y donde juega un papel importante el uso de los llamados Métodos de Expertos.[35]

. Entre los métodos para las validaciones de las investigaciones se encuentran

- Brain Storming.
- Grupos Nominales.
- Método Delphi.

Para validar la propuesta se ha seleccionado el método del criterio de expertos, para lo cual la autora decide acotar que solicitó la concurrencia de personal calificado como especialista en temas informáticos.

Dentro de los sistema de expertos no estructurados se seleccionó para desarrollar el proceso el método Delphi, el cual pretende extraer y maximizar las ventajas que presentan los métodos basados en grupos de expertos y minimizar sus inconvenientes. Para ello se aprovecha la sinergia del debate en el grupo y se eliminan las interacciones sociales indeseables que existen dentro de todo grupo. De esta forma se espera obtener un consenso lo más fiable posible del grupo de expertos.

El método Delfhi, (Landeta.,1999) cuyo nombre se inspira en el antiguo oráculo de Delphos, parece

[35] Cortés, Cortés, Manuel E. y otros. Generalidades sobre Metodología de la Investigación. UNACAR. México. 2005. p.

que fue ideado originalmente a comienzos de los años 50 en el seno del Centro de Investigación estadounidense RAND Corporation por Olaf Helmer y Theodore J. Gordon, como un instrumento para realizar predicciones sobre un caso de catástrofe nuclear. Desde entonces ha sido utilizado frecuentemente como sistema para obtener información sobre el futuro.

El método Delphi consiste en la selección de un grupo de expertos a los que se les pregunta su opinión sobre cuestiones referidas a acontecimientos del futuro. Las estimaciones de los expertos se realizan en sucesivas rondas, anónimas, al objeto de tratar de conseguir consenso, pero con la máxima autonomía por parte de los participantes.

Por lo tanto, la capacidad de predicción del Delphi se basa en la utilización sistemática de un juicio intuitivo emitido por un grupo de expertos.

Es decir, el método Delphi procede por medio de la interrogación a expertos con la ayuda de cuestionarios sucesivos, a fin de poner de manifiesto convergencias de opiniones y deducir eventuales consensos. La encuesta se lleva a cabo de una manera anónima (actualmente es habitual realizarla haciendo uso del correo electrónico o mediante cuestionarios Web establecidos).

El conjunto de opiniones que se obtiene de la consulta es sometido a un análisis. Los resultados que se obtengan son enviados a los expertos nuevamente con el objetivo de que puedan modificar si así lo estiman conveniente las opiniones anteriormente dadas, a partir de conocer el criterio de sus colegas expertos. Este procedimiento se aplica tantas veces como sea necesario hasta obtener por parte del modelador un consenso de los criterios de los expertos.

Las preguntas se refieren, por ejemplo, a las probabilidades de realización de hipótesis o de acontecimientos con relación al tema de estudio. La calidad de los resultados depende, sobre todo, del cuidado que se ponga en la elaboración del cuestionario y en la elección de los expertos consultados.

En la familia de los métodos de pronóstico, habitualmente se clasifica al método Delphi dentro de los métodos cualitativos o subjetivos.

La aplicación de este método plantea los requisitos siguientes:

♣ *El anonimato de los expertos.*

Puesto que se les da a conocer los resultados de las rondas de respuestas de ellos, el no conocimiento de quiénes son los que respondieron, elimina las posibles influencias de aquellos que pudieran ser considerados más conocedores del tema en cuestión.

♣ *La retroalimentación controlada.*

Esto significa que una vez obtenidas las respuestas de la ronda de preguntas, deben ser totalmente procesadas de forma tal que se les ofrezca nuevamente a los expertos para que conozcan los criterios de los otros encuestados sobre las propias preguntas a él formuladas.

Lo que permite al experto revisar su valoración y mantenerla o modificarla en la próxima ronda de preguntas. Este proceso se debe realizar cada vez que se considere llevar a vías de hecho una nueva consulta.

♣ *La respuesta estadística de grupo.*

El mantener un procesamiento estadístico de los resultados de cada una de las rondas les va permitiendo a los investigadores conocer la evolución de las respuestas de los encuestados lo que les permitirá sacar conclusiones finales de la temática que están abordando.

Por otra parte se considera muy poderoso el hecho de que las decisiones finales que tomen los investigadores estén avaladas por los resultados de las opiniones consensuadas de un grupo de personas considerados como expertos en la materia que se trate.

Las características esenciales de los expertos, estarán dadas por los indicadores siguientes:

- Competencia,
- Creatividad,
- Disposición a participar en la encuesta,
- Capacidad de análisis y de pensamiento,
- Espíritu colectivista y autocrítico.

Es importante destacar la tendencia a considerar a una persona experta a partir de su grado científico, título académico o cargo que ocupa. Sin embargo, estas condiciones algunas veces no determinan la competencia de una persona. La competencia de un experto se podrá considerar a partir de la valoración que se realice del nivel de calificación que posea en una determinada esfera del conocimiento y se puede medir a partir de obtener el coeficiente k, que se calcula mediante la fórmula siguiente:

$K = 1/2(kc + ka)$

Donde *kc*, es el coeficiente de conocimiento que tiene el experto sobre la temática que se aborda, el

cual se calcula mediante la autovaloración del propio experto en una escala del 0 al 10 y multiplicado por 0.1

Para cada experto se obtiene su coeficiente de conocimiento kc sobre el tema. De esta forma el resultado que se obtuvo fue el siguiente:

Experto No.	Coeficiente *Kc.*
1	1,0
2	0.9
3	1.0
4	0,9
5	0.8
6	1.0
7	0,8

Para calcular el coeficiente de argumentación o fundamentación *ka*, se empleó la tabla patrón siguiente, donde cada experto indicó las fuentes que consideró de mayor influencia sobre el tema.

Fuentes de argumentación	Grado de influencia de cada una de las fuentes según sus criterios		
	Alto	Medio	Bajo
1. Análisis teóricos realizados por usted.	0,2	0,15	0,05
2. Experiencia obtenida en la actividad de auditoria de	0,4	0,35	0,25

las TI			
3.Experiencia obtenida como auditor del sistema.	0,3	0,25	0,15
4.Su intuición	0,1	0,05	0,05

Seguidamente se sumaron todos los valores obtenidos y ese resultado formó el coeficiente de argumentación *ka* de cada experto.

Teniendo como datos los coeficientes de conocimientos *kc* y de argumentación *ka* , se calcula el coeficiente de competencia de cada experto (*K*) .

El código para la interpretación del coeficiente de competencia (*K*) es el siguiente:

Si $0.8 < K < 1.0$ entonces el coeficiente de competencia es alto

Si $0.5 < K < 0.8$ entonces el coeficiente de competencia es medio

Si $K < 0.5$ entonces el coeficiente de competencia es bajo

De este modo, se obtiene para los expertos:

1) $K = 1/2 \quad (1{,}0 + 0{,}75) = 0{,}875$

2) $K = 1/2\ (0{,}9 + 0{,}85) = 0{,}875$

3) $K = 1/2 = (1.0 + 0{,}85) = 0{,}925$

4) $K = 1/2\ (0{,}9 + 0{,}85) = 0{,}875$

5) $K = 1\ /2\ (0.8 + 0{,}95) = 0{,}875$

6) $K = 1\ /2\ (1.0 + 0{,}8) = 0{,}9$

7) $K = 1/2\ (0.8 + 0{,}9) = 0{,}85$

Como se puede observar el grado de competencia es ***alto.***

Para medir el grado de concordancia de los expertos teniendo en cuenta todas las preguntas e indicadores se utiliza el coeficiente de concordancia de Kendall o coeficiente de correlación de rango.

El coeficiente se define así:

Coeficiente de Kendall

$$K = \frac{12\sum_{j=1}^{n}(S_j - \bar{S})^2}{m^2(n^3 - n) - m\sum_{i=1}^{m} T_i}$$

Recomendado para emplear cuando $n > 7$, donde:

m: número de expertos.

n: número de preguntas o indicadores.

$S_j = \sum_{i=1}^{m} R_{ij}$ donde R_{ij} es el rango asociado a la evaluación del experto i a la pregunta j

$\bar{S} = \frac{\sum_{j=1}^{n} S_j}{n}$ es la media y

T_l es el resultado de los rangos iguales llamados ligaduras que ofreció el experto i para las preguntas

$T_l = \frac{\sum_{i=1}^{l}(t^3 - t)}{12}$ donde l : número de grupos con rangos iguales para el experto i

t : número de observaciones dentro de cada uno de los grupos para el experto i

Se procede a plantear entonces las siguientes hipótesis estadísticas:

H0: No existe concordancia entre los expertos (**)

H1: Existe concordancia

3.2. Proceso de validación realizado.

Concepción inicial del problema:

Se definen los elementos básicos del trabajo, el objetivo a alcanzar, la situación actual y los componentes o elementos necesarios para llevar a cabo el trabajo.

Selección de los expertos:

Se determinan la cantidad de expertos, estableciendo determinadas pautas que avalen su experiencia, prestigio y conocimiento científico.

Elaboración y aplicación de los cuestionarios:

Una vez conformado el universo de los expertos se elabora un primer cuestionario, teniendo en cuenta los elementos comunes en cada una de las respuestas se elabora con estos una segunda ronda de cuestionarios con preguntas cerradas, las que permiten arribar a cuestiones generales con las que se confecciona una última encuesta.

Las preguntas se hacen por escrito y se responden de forma independiente, para evitar la influencia de un experto sobre otro.

Procesamiento y análisis de información:

Se toman en consideración el sistema de preguntas aplicadas en cada una de las rondas y se tabulan estadísticamente.

Se hace necesario plantear como un criterio generalizado de varios autores, que dentro de la ciencia informática se hace complejo la determinación de la competencia de personal catalogado como experto, pues se considera aún una ciencia joven; por lo que a partir de esta reflexión se comenzará a denominar genéricamente como expertos al personal considerado como especialista en esta rama del saber.

3.2.1. Metodología utilizada para la validación de la guía para la evaluación del Sistema de Control Interno a las Tecnologías Informáticas.

Etapas y tareas del proceso de validación

La validación se realizó en tres etapas: en la primera se seleccionaron los especialistas de acuerdo con los criterios establecidos, en la segunda se elaboraron y aplicaron los cuestionarios de opiniones a los especialistas, en la tercera se procesaron los resultados de las valoraciones emitidas por los especialistas.

Selección de los especialistas:

Dadas las características de esta investigación se decidió seleccionar un grupo de especialistas integrado por profesionales especializados en Informática Educativa y en Seguridad Informática, para valorar críticamente la multimedia elaborada.

La selección de especialistas se realizó atendiendo a los siguientes criterios:

- Competencia, expresado en su nivel de conocimiento acerca del problema que se resolvió con el producto.
- Creatividad expresada en su capacidad para resolver problemas originales.
- Disposición para participar en la validación.
- Capacidad de análisis y de pensamiento lógico.
- Espíritu colectivista y autocrítica.

Después de determinar la cantidad mínima y máxima de especialistas que podían participar en la investigación, se confeccionó el listado definitivo.

El próximo paso fue enviar a cada uno de los especialistas una carta invitándolos a participar en el peritaje en la cual se le explicó el objetivo de la realización de la encuesta, el plazo y el orden de ejecución, así como el volumen total del trabajo. En dicha carta se le envió una encuesta sobre su competencia y algunos datos personales.

Para la determinación del nivel de competencia se utilizó la autovaloración de los mismos, utilizando la metodología elaborada y aprobada por el Comité Estatal de Ciencia y Técnica de la antigua URSS, la cual consiste en la determinación del coeficiente *k* de competencia.

Elaboración a aplicación de los cuestionarios.

Como ya se ha expuesto antes uno de los elementos metodológicos que debe poseer la aplicación práctica del método son los cuestionarios.

Este cuestionario tiene la particularidad de que está confeccionado de manera que los expertos seleccionados ofrecen su opinión sobre cada una de las etapas a través de 5 categorías evaluativas. (Ver documentos anexos)

5.- Muy adecuada (MA)

4.- Bastante adecuada (BA)

3.- Adecuada (A)

2.- Poco adecuada (PA)

1.- No adecuada (NA)

El cuestionario fue sometido a 7 expertos seleccionados.

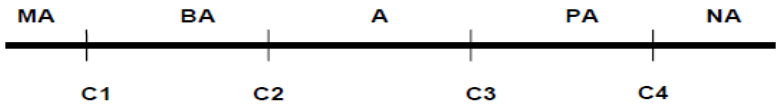
Procesamiento de los resultados.

En este paso se tuvo en cuenta las respuestas a cada una de las preguntas que aparecen en el cuestionario, así como la coincidencia o no de las mismas, resaltando aquellos criterios que puedan enriquecer o mejorar la resultante de la investigación.

El procesamiento estadístico de los datos y el análisis de las respuestas realizadas por los expertos, permitió apreciar el consenso de estos, de acuerdo a las hipótesis establecidas anteriormente (**). Al procesar las respuestas empleando el paquete SPSS, dado que α=0.05 > Sig. asőtt .= 0,0016 se rechaza Ho y por tanto puede arribarse a la conclusión que existe concordancia entre los expertos con un nivel de significación del 5%.

Luego se establecen los denominados puntos de corte (del C1 al C4) que se hacen corresponder con las 5 categorías evaluativas:

Si las categorías evaluativos son ($n \in N$) entonces los puntos de corte son n-1



Posteriormente se realizan los siguientes pasos:

1er Paso. Construir una tabla de frecuencias acumuladas

2do Paso. Construir una tabla de frecuencias relativas acumuladas

3er Paso. Buscar una imagen de cada uno de los valores de las celdas de la tabla anterior, mediante la inversa de la curva normal.

Tabla resumen

Indicadores	5	4	3	2	1	Total
1	3	4	3	-	-	7
2	5	1	-	-	-	7
3	7	3	-	-	-	7
4	5	3	2	-	-	7
5	5	3	2	-	-	7
6	5	3	2	-	-	7
7	6	4	-	-	-	7

Tabla de frecuencias acumuladas

Indicadores	5	4	3
1	3	7	7
2	6	7	-
3	7	7	-
4	5	6	7
5	5	7	7
6	5	7	7
7	6	7	-

Tabla de frecuencias relativas

Indicadores	5	4	3
1	0,30	0,70	1,00
2	0,60	0,70	-
3	0,70	0,70	-
4	0,50	0,60	1,00
5	0,50	0,70	1,00
6	0,50	0,70	1,00
7	0,60	0,70	-

Tabla de inversa a la curva normal

Indicadores	5	4	3	Sumas	Promedio (P)	N-P
1	-0,5244	0,5244	3,49	3,49	1,16	0,02
2	1,2815	3,49	-	4,77	1,59	-0,41
3	0,5244	3,49	-	4,01	1,34	-0.16
4	-1,3921	0,8416	3,49	2,94	0,98	0,2
5	-1,3921	0,8416	3,49	2,94	0,98	0,2
6	-1,3921	0,8416	3,49	2,94	0,98	0,2
7	0,2533	3,49	-	3,74	1,25	-0,07
Puntos de Corte	0,26	1,75	3,49	24,83		

Los puntos de corte se obtienen al dividir la suma de los valores correspondientes a cada columna entre el número de aspectos a evaluar.

N – *P*, se determina de la forma siguiente:

$$N = \frac{Total\ de\ la\ suma}{\text{indicadores} \,.\, \text{categorías}} = \frac{24{,}83}{7.3} = 1{,}18$$

Por tanto, *N* − *P*, es el valor promedio que le otorgan los expertos a cada etapa del procedimiento.

Los puntos de corte sirven para determinar la categoría o grado de adecuación de cada etapa del procedimiento según la opinión de los expertos consultados.

Como los resultados N – P están situados a la izquierda del punto de corte que separa la categoría muy adecuado de la de bastante adecuado, se puede afirmar que todos los indicadores que aparecen en el primer bloque quedan evaluados de muy adecuados (muy altos) por el 98 % de los encuestados. Por lo que se puede determinar que la guía elaborada cumple las exigencias planteadas para el objetivo propuesto.

3.3. Conclusiones parciales

Del análisis de los resultados del cuestionario y los argumentos ofrecidos por los especialistas se puede resumir que:

1.- La estructuración del cuestionario permitió hacer un análisis con profundidad de aquellos aspectos de más relevancia de la guía.

2.- De forma general la guía y la estructura que sustenta, fue evaluado de aceptable por el 89,4 % de los expertos.

3.- Las orientaciones metodológicas presentadas permiten optimizar el desempeño de los auditores del sistema.

Tomando como base el procesamiento del cuestionario y el análisis de valoraciones escritas se pueden plantear que la guía permite hacer una evaluación eficiente del sistema de control interno de las TI, lo que la convierte en un instrumento óptimo para el trabajo de los auditores en ejercicio del sistema de auditoria.

CONCLUSIONES

Luego de concluido el proceso de investigación se puede aseverar que se alcanzó el objetivo trazado, por lo que de manera conclusiva general se expresa lo siguiente:

1. La guía metodológica diseñada constituye un instrumento óptimo para el trabajo de los auditores en ejercicio del sistema de auditoria en los temas relacionados con la revisión del sistema de control interno de las TI.

2. La guía se estructura y sustenta en las resoluciones vigentes, lo que permite verificar el cumplimiento de lo establecido referente a los recursos de las tecnologías de la información y sus servicios asociados, mejorando el sistema evaluación del control interno de la actividad informática de las organizaciones.

3. El proceso de validación permitió comprobar que es necesario y posible el uso de la guía metodológica dentro de las acciones de control que realiza el Sistema de Auditoría relacionada con las TI.

RECOMENDACIONES

1.- Aplicar la Guía de Evaluación al Control Interno de las Tecnologías de la Información.

2.- Capacitar a los auditores del Sistema con los referentes necesarios para la implementación de la guía.

BIBLIOGRAFÍA

Arima Ideo, Carlos. (2002). *Auditoría contra fraudes de sistema informatizados.*

Armada Trabas, Elvira. (2005). *El Control interno en Cuba. Realidad empresarial. Vínculo con la auditoría.*

Asamblea Nacional del Poder Popular. (2009, August 1). Decreto Ley No. 107 " Ley de la Contraloría General de la República de Cuba".

Bejerano Portela, Gladys. (2010). Indicaciones Generales para la Guía de Autocontrol Interno. La Habana.

Blanco Encinosa, Lázaro. (2001). *El control interno en los sistemas informáticos de las pequeñas y medianas empresas*.

Capote Cordovés G. (2001). El control interno y el control. Economía y Desarrollo. Retrieved from http://www.dict.uh.cu/Revistas/economia_desarrollo/2001n- 2/GabrielCapote.pdf.

Carballosa Rodríguez, Dulce. (2010). *Adecuación de la guía de auto- control interno al sector de la salud en la provincia de Cienfuegos*.

Comité Ejecutivo del Consejo de Ministros. (2002). Acuerdo No. 4374.

Consejo Auditoria y Control Interno. (2004). Retrieved from http://www.gestiopolis.com.htm.

Contraloría General de la República. (2011). Resolución No.60 "Control Interno".

Contraloría General de la República. (2010). VI Comprobación Nacional al Control Interno. Actividad Presupuestada 2010.

Control Interno una responsabilidad de todos los integrantes. (2005). . Retrieved from http://www.gestipolis.com.

Cook y Winkle. (2006). *Auditoría*.

Delgado García, Alfa Iris. (2006). *Procedimiento para la elaboración de la estrategia de Control Interno a partir de la Matriz DAFO.*

Estrada Sevilla, Mayra. (2006). *Metodología para documentar los sistemas de control interno bajo el enfoque administrativo*.

Fernández Riverón, Tania. (2009). Impacto de la Auditoría a las Tecnologías de la Información en la corporación Copextel S.A.

García Cabrera. Gerardo. (2002). *De la Era de la Información a la Sociedad del Conocimiento. En Ciencia, Innovación y Desarrollo* (Vol. 6).

García Pino, René. (2009). El Control Interno y los Sistemas Automatizados para la Gestión Económica. Retrieved from http://www.gestiopolis.com.htm.

González, María. (2005). Control Interno. Retrieved from http://gestiopolis.com/recursos/documentos/fulldocs/fin/ctinmegp.htm.

Los Sistemas de Control Interno. (2011a). Retrieved from http://www.eleconomista.cubaweb.cu.cuba.

Los Sistemas de Control Interno. (2011b). Retrieved from http://www.coso.org.estadosunidos.

Los Sistemas de Control Interno. (2011c). Retrieved from http://www.gestiopolis.com.mexico.

Martínez Calderín, Leidisara. (2011). *El control interno: Un medio eficaz para la toma de decisiones en el control de la gestión.*

Ministerio de Auditoria y Control. (, 95/06/08). Decreto Ley No.159 "Norma la actividad de auditoria y establece sus principios fundamentales".

Ministerio de Auditoria y Control. (2010). Normas para los auditores gubernamentales. Retrieved from http://www.bibliociencias.cu/gsdl/collect/revistas/index/assoc/HASH6e54/32a38a83.dir/doc.pdf.

Ministerio de Auditoría y Control. (2002). *Manual del Auditor, "Auditoría a las TICs"*. Ciudad de La Habana.

Ministerio de Auditoría y Control. (2007). Resolución No.350.

Ministerio de Informática y las Comunicaciones. (2007). Acuerdo No.6058.

Moreno Montaña, Eliana. (2011). Auditoría. Retrieved from http://www.gestiopolis.com/recursos/documentos/fulldoc/fin1/auditeliana.htm.

Pérez Campaña, Marisol. (2011). El Sistema de Gestión. Conceptos básicos para su diseño. Retrieved from http://wwwgestiopolis.com/canales/gerencial/articulos/67/siscontrges.

Regla Caridad Montejil, Rogers. (2007). El sistema de Control Interno sus retos y vivencias. *Revista Auditoria y Control*.

Sophos: Informe anual de seguridad 2005. (2005). . Retrieved from http://www.cucert.co.cu/lectu.php

ANEXOS

Anexo No. 1

Guía PROCEDIMIENTOS DE VERIFICACIÓN PARA EL AUDITOR

Nº.	COMPROBAR, VERIFICAR E INVESTIGAR, SI:	RESPUESTAS			
	TEMAS O ASPECTOS A AUDITAR.	SI	NO	PT#	COMPROBACION
•	**CONTROLES Y MEDIDAS**				
➢	La entidad cuenta con un sistema de salva sistemática y oportuna de la información				
➢	Se conserva una segunda salva en otro local (no sólo para los datos sino para el software básico y de aplicación y la documentación)				
➢	Existe la definición y creación de condiciones para un centro de procesamiento alternativo				
➢	Existen las condiciones requeridas para la conservación de los soportes magnéticos e identificación de los mismos				
➢	Existen los Dispositivos de Seguridad Física (para el disco duro, torres de disquete, etc.,) según se requiera y/o esté planteado en el PSI.				
•	Existe la designación del (los) responsable(s) y activista(s) de Seguridad Informática, de la entidad y por área según se requiera.				
•	Existe conocimiento por parte de los implicados de las medidas de PSI y el PC en las que están implicados y preparación para darle cumplimiento (incluido los responsables y activistas de SI)				
•	Comprobar la No utilización de antivirus o utilización de antivirus inadecuados				
•	Existe indisciplina en la actualización de los antivirus				
•	Existe el adecuado control de acceso a los locales				
•	Están creadas las condiciones, según los requerimientos de las áreas donde están ubicados los medios (climatización inadecuada, deficiencias constructivas, elevado nivel de polvo, etc.)				
•	Se garantiza el aterramiento				
•	Se garantiza el Backup adecuado				
•	Señalización de las tomas eléctricas				
•	Existen las medidas de protección contra incendios definidas para los lugares con este tipo de medios técnicos.				
•	Existe la Cuarentena técnica para el software adquirido por vía no estrictamente confiable				

Nº.	COMPROBAR, VERIFICAR E INVESTIGAR, SI:	RESPUESTAS			
	TEMAS O ASPECTOS A AUDITAR.	SI	NO	PT#	COMPROBACION
•	Es correcta la utilización de los productos antivirus los cuales deben estar certificados y actualizados				
•	Existe la políticas de protección contra programas dañinos (ej. Abrir sin macro, no abrir adjuntos de correo de procedencia dudosa en equipos con información sensible)				
•	Existe la documentación requerida (de aplicaciones, software base, medios técnicos, etc.)				
•	Existe la Reglamentación adecuada de la información a trasmitir y control de su cumplimiento				
•	Comprobar la creación de las trazas requeridas y chequeo sistemático de las mismas				
•	**Passwords** – Garantizar la utilización de los mismos de acuerdo a los requerimientos, Estructura, de los passwords – Establecerlos para el acceso al equipo (setup), acceso a la red, acceso a las aplicaciones y a sus opciones de acuerdo a los requerimientos – Conservación en sobre sellado de las claves para su uso por el personal autorizado en caso necesario y correcta definición del procedimiento de acceso a las mismas. – Procedimientos adecuados para la actualización de las claves – Utilización y control de accesos de emergencia.				
2.	**DOCUMENTACION**				
•	Verificar que estén actualizados los Manuales de Usuario de las Aplicaciones que explotan.				
•	Verificar que estén documentadas adecuadamente las aplicaciones que hayan desarrollado y/o los programas elaborados, así como a soluciones incorporadas a aplicaciones en explotación. Tanto la referida al desarrollo de la aplicación (Diseño y Programación) como el Manual de Usuario. La primera de modo que sea factible su mantenimiento y actualización por personal informático aunque no haya participado en su diseño.				
•	Verificar que cuenten con documentación de la tecnología adquirida.				

Nº.	COMPROBAR, VERIFICAR E INVESTIGAR, SI:	RESPUESTAS			
	TEMAS O ASPECTOS A AUDITAR.	SI	NO	PT#	COMPROBACION
3.	**SEGURIDAD INFORMATICA**				
3.1	Existe el Plan de Seguridad Informática (PSI) y de Contingencias (PC) y evaluarlo				
3.2	Comprobar que el PSI esté debidamente actualizado				
3.3	Existe la designación de él (los) responsable(s) de Seguridad Informática y preparación y conocimiento de los mismos para realizar sus funciones.				
3.4	Evaluar el tratamiento que se dé al procesamiento mediante tecnologías de la información y las comunicaciones a la información sensible y clasificada.				
3.5	Verificar que el PSI garantice el tratamiento adecuado a la información sensible, según los requerimientos de la entidad				
3.6	Verificar que el PSI garantice el tratamiento que la resolución 6/96 del MININT, resolución 204/96 del SIME, Resolución CEF-INSAC (aún vigente) y otros documentos normativos generales o corporativos plantean para este tipo de información.				
3.7	Existe el Análisis de dualidad de funciones que afecten la Seguridad Informática y en general el correcto funcionamiento del sistema informático de la entidad. Delimitación de funciones y responsabilidades. Ej. Coincidencia entre Jefe de informática, con el responsable de SI y/o con el administrador de la red.				
3.8	Verificar que las políticas controles y medidas plasmados en el mismo se correspondan con la evaluación de riesgos realizada por la entidad y/o por los auditores durante la exploración				
3.9	Verificar que el PSI o en su defecto las medidas implantadas se correspondan con el Reglamento de Seguridad Informática del MININT, con el Reglamento para la Protección y Seguridad Técnica de los sistemas Informáticos del SIME y con las normativas y regulaciones corporativas existentes.				
3.10	Verificar si se realiza la supervisión del cumplimiento de lo establecido en el PSI y en el PC o en su defecto en el cumplimiento del sistema de medidas establecidas en la entidad al respecto.				
3.11	Existe un registro de las violaciones detectadas y se chequean las medidas adoptadas.				
3.12	Verificar si está correctamente habilitado el control de acceso				

Nº.	COMPROBAR, VERIFICAR E INVESTIGAR, SI:	RESPUESTAS			
	TEMAS O ASPECTOS A AUDITAR.	SI	NO	PT#	COMPROBACION
3.13	Verificar si el acceso establecido a aplicaciones, redes y otro servicios se corresponde con lo establecido. Es decir si los que tienen acceso son los que lo deben tener y si tienen el tipo de acceso que les corresponde.				
3.14	Verificar la actualización y eficacia de los productos antivirus				
3.15	Se realiza la salva de la información con la sistematicidad y el número de copias requeridos.				
3.16	Existe la identificación de los soportes magnéticos que contienen las salvas.				
3.17	Verificar la conservación de la salva de la información sensible en otro recinto o edificación.				
3.18	Verificar la existencia de lugares de procesamiento alternativo y otras medidas orientadas a garantizar la continuidad de los procesos.				
4.	**SOFTWARE**				
4.1	Existe la información sobre los Sistemas Operativos con que se trabaja, versiones				
4.2	Verificar si las aplicaciones corporativas que se explotan en la entidad se corresponden con las última versiones				
4.3	Evaluar si están instaladas aplicaciones o utilitarios que permitan modificar las aplicaciones o vulnerar la seguridad				
4.4	Si existen aplicaciones adquiridas o elaboradas en la propia entidad, verificar: ➢ Están aprobadas por DATACIMEX ➢ Poseen trazas de auditoría ➢ Poseen claves de acceso ➢ Las bases de datos asociadas están encriptadas				
5.	**OTROS ASPECTOS**				
5.1	Verificar la planificación, ejecución del mantenimiento a los equipos				
5.2	Existen las condiciones ambientales de los lugares donde están ubicados los equipos				
5.3	Existe la garantía de fuente de energía eléctrica y control de voltaje para los medios técnicos asociados a la informática y las comunicaciones.				
5.4	Verificar la existencia de tierra física.				

Anexo No. 2
GUIA

1. Revisión de la existencia de un sistema de Seguridad Informática.

En las comprobaciones a realizar, se debe verificar que la entidad tenga diseñado e implementado un Sistema de Seguridad Informática, a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos. A Partir de éste deben elaborar el Plan de Seguridad Informática y Contingencia y análisis de riesgo y entre los documentos bases a utilizar debe estar la Resolución 6/96 del MININT y 127/07 del MIC.

- Confirmar existencia del Plan de Seguridad y Contingencias. Análisis de riesgos para los activos informáticos
- Debe estar designado un responsable de seguridad informática y no puede ser el administrador de la red.
- Debe estar registrado en el plan, sus últimas actualizaciones.
- Existencia de un registro de incidencias en cada área donde existan activos informáticos, en el cual se registrara la incidencia que ocurra con cada activo.

En el plan:

- Medidas de recuperación ante Contingencias (Contaminación Virus Informático, destrucción de información almacenada, acceso no autorizado, modificación de información, fallas de fluido eléctrico, fallas de hardware, Incendios, desastres naturales, Hurtos.)
- Registro con nombres de usuarios con acceso al correo electrónico e Internet.(Uso personal de las contraseñas)
- Registros (Control de soporte y salvas, auditorias realizadas, Entrada Salida y movimiento de tecnología de información, Incidencias, trabajo en maquina, mantenimiento o reparación de roturas.).
- Procedimiento para el uso de los registros.
- Procedimientos de contingencia
- (Ver índice Impreso)

2. Clasificación y control de los bienes informáticos.

- Mantener actualizado el inventario de las tecnologías informáticas. (Resolución 127/07, artículo 14 sección primera)

- Mantener actualizado expediente técnico de las PC.(Incluye los componentes y especificaciones técnicas de las pc y lo debe tener el responsable de cada local o maquina) Resolución 127/07.
- Cada uno de los bienes informáticos debe estar bajo la custodia documentada legalmente de un especialista.(Resolución 127/07).(Actas de responsabilidad).
- Existencia de un plan de mantenimiento.
- Verificación de las actas de mantenimiento y reparaciones (Dependencia, Fecha, Nombre y Apellidos del Visitante, PC a recibir el mantenimiento, los materiales utilizados, materiales entregados, mano de obra, descripción del trabajo, el nombre y apellidos, la fecha en que se ejecuta el trabajo y el nombre y apellidos del ejecutante, fecha y firma de la persona que recibe el servicio).

3. Seguridad física y ambiental de los locales.

Señalizar el voltaje en los tomacorrientes y en las tecnologías informáticas.

- Velar porque los locales en los que se encuentran las tecnologías informáticas sean seguros y con sello en las puertas.
- Limitar el acceso físico a los servidores.
- Conectar las computadoras a fuentes de respaldo de energía con limitadores de voltaje.
- Verificar que se encuentren selladas todas las PC.

4. Comprobar la Identificación, autenticación y control de accesos.

- Uso de contraseñas para el acceso al sistema, personales y únicos, verificar permisos de usuarios.
- Cambio de contraseñas frecuentemente.

5. Comprobar la seguridad ante programas malignos.

- Verificar antivirus instalado y frecuencia de actualización.(resolución No. 204/96 del SIME en su ARTICULO 27)
- Medidas para evitar infecciones, (implementar un Firewall en la conf de la red, no abrir correos de procedencia dudosa).

6. Comprobar la existencia de Respaldo de la información.

- Salvas de los sistemas operativos y programas usados en la entidad.(Copias en servidores, CD, y en otros lugares apartados de los servidores).

7. Comprobar la Seguridad en redes.

- Implementar mecanismos de seguridad en la red que permitan depurar o filtrar información ()

- Garantizar protección a servidores y terminales, tener elementos que permitan el monitorio y la auditoria de l os principales eventos que ocurren en la red. ().
- Existencia de un administrador de la red.
- Existencia de sitios web en servidores fuera del país o cuentas de correo.
- Certificación de las redes (Resolución 65/03 del MIC).

8. Sistemas Contables financieros.

- Nombrar el o los sistemas contables que se utilizan y los módulos que tiene.
- Verificar que los sistemas contables estén certificados. (Solicitar copia de dicha certificación.) Resolución Conjunta MFP-MIC.
- Contrato de mantenimiento. (Actualización de versión o problemas técnicos.)
- Verificar que la entrada al sistema este protegida por contraseñas y estén definidas a varios niveles de acceso.
- Ver listados del nivel de acceso de los usuarios.()
- Ver manual de usuario.
- Ver registro y control de los soporte y salvas actualizado. Cumpliendo así lo establecido en la resolución No. 6/96 MININT en su ARTICULO 31.. (En cd, servidores u otras pc alejadas del local central).

9. Empresas con servicio de Internet:

- Revisar el acta de compromiso de los usuarios de Internet.
- Revisar que existan en las áreas o locales autorizados a la navegación en Internet las normas y reglamentos para el uso de la misma.
- Comprobar la posibilidad de envió de correos sin autentificación. (Verificar el tipo de correo que utilizan y si pide autentificación a la hora de entrar o enviar mensajes.)

Anexo No. 3

No.	Aspectos a controlar	Artículo	Sí	No	NP
Sistema de Seguridad Informática					
Diseño del Sistema de Seguridad Informática.					
1.1	¿En los Consejos de Dirección o instancia equivalente se analizan temáticas sobre la seguridad de las tecnologías de la información y se deja constancia escrita en las actas?	Acuerdo 6058 CECM inc. 4to			
1.2	¿Se realizó el análisis de riesgo a partir de la importancia de los bienes informáticos a proteger? ❖ Se identificaron correctamente las amenazas. ❖ Se definieron los bienes informáticos de mayor importancia y niveles de riesgos. ❖ El resultado final del análisis de riesgo se corresponde con lo detectado durante el control.	Art. 4			
1.3	¿El sistema de seguridad informática diseñado se corresponde con los riesgos a que están sometidos y persigue minimizarlos, garantizando la continuidad de los procesos? ❖ ¿Las políticas y medidas de seguridad definidas están dirigidas a minimizar los riesgos? ❖ ¿Las políticas y medidas de seguridad implementadas en la práctica se corresponden con las definidas en el sistema de seguridad informática diseñado? ❖ ¿Se realizan actualizaciones sistemáticas del sistema de seguridad, atendiendo la identificación de nuevos riesgos o la ocurrencia de incidentes de seguridad? ❖ ¿Existen procedimientos ante contingencias, que garanticen una adecuada restauración del servicio con la pérdida mínima de datos? ❖ ¿Están definidos los recursos y responsables de garantizar la continuidad de los procesos ante cualquier	Art. 4			

	eventualidad o incidente de seguridad? ❖ ¿Existen evidencias documentales sobre la realización de pruebas dinámicas para comprobar la efectividad del plan de recuperación?				
1.4	¿Existen registros para dejar constancia escrita de las principales incidencias que ocurren, realización de las salvas de información, control de entrada y salida de bienes informáticos?	Art. 4			
1.5	¿Se tiene elaborado el plan de seguridad informática como expresión gráfica del sistema diseñado?	Art. 5			
1.6	¿El plan de seguridad informática se encuentra actualizado? Comprobar que: ➢ ¿Se encuentra aprobado por el máximo dirigente de la entidad? ➢ ¿Su fecha de elaboración es posterior a la puesta en vigor de la Resolución 127 del MIC (24 de Julio del 2007)? ➢ ¿La caracterización del entorno informático y la definición de los servicios se corresponde con lo existente en la práctica? ➢ ¿Se definen políticas de seguridad que respondan a la minimización de los riesgos identificados y están implementadas? ➢ ¿Se tienen elaborados los procedimientos y acciones a realizar ante la ocurrencia de incidentes o violaciones de seguridad?	Acuerdo 6058 CECM Art. 7, 9 inc b), 10 inc a) y 62 inc f)			
Funciones y Responsabilidades de Seguridad Informática.					
1.7	¿Se tienen definidas las responsabilidades y obligaciones sobre la Seguridad Informática según los cargos que ocupan? ❖ Máximo dirigente de la entidad ❖ Especialistas de seguridad informática ❖ Jefe Departamentos ❖ Jefe Departamento Informática ❖ Administrador de la red ❖ Usuarios de las tecnologías ❖ Diseñadores de aplicaciones informáticas y Web.	Acuerdo 6058 CECM Art. 9, 8, 9, 10, 62 11 y 12			
	Existe un adecuado conocimiento y conciencia de la Seguridad Informática por parte de la alta				

	dirección de la organización como máxima responsable del tema.				
1.8	¿Los jefes a las diferentes instancias divulgan a los trabajadores sobre sus deberes, derechos, políticas y procedimientos en relación con el sistema de seguridad informática?	Art. 9 inc d), 10 inc g) y 22			
1.9	¿Los usuarios de las tecnologías informáticas tienen conocimiento de las regulaciones, medidas, deberes, derechos, procedimientos y políticas con relación al sistema de seguridad informática y el empleo de sus servicios.	Art. 12 inc a), 22 y 65			
1.10	¿Existe constancia documental sobre la realización de controles a la seguridad informática por los Especialistas de los Organismos, Grupos o Direcciones Nacionales?	Art. 8			
1.11	¿Se tienen evidencias documentales sobre la realización de controles internos de seguridad informática que garanticen la supervisión sistemática sobre el empleo de las tecnologías y sus servicios? ❖ ¿Se planifican los controles de seguridad informática? ❖ ¿Dejan constancia escrita sobre los resultados de los controles? ❖ ¿Se informan los resultados a la máxima dirección e instancias pertinentes? ❖ ¿Son comprobaciones profundas o dirigidas a temas específicos?	Art. 9 inc d), 10 inc b), inc e) y 21			
1.13	¿Existe constancia escrita sobre los procesos de selección y verificación del personal que ocupa los cargos vinculados a la actividad informática (Jefe de departamento, administradores de red e informático) incluyendo personal eventual o estudiantes con accesos a sistemas críticos, información de valor o se dedican a la supervisión y seguridad de los sistemas?	Art. 18			
1.14	¿Los términos y condiciones del contrato de empleo incluyen la obligación de la entidad contratante en cuanto a la preparación del contratado, así como la responsabilidad del trabajador hacia la seguridad informática, especificando que estos requerimientos	Art. 19			

	mantienen su vigencia una vez finalizada la relación laboral?				
1.15	¿Se tienen definidas de forma explícita las violaciones de seguridad informática y las medidas disciplinarias que se adoptaran? Entre otras: • Uso no autorizado de las tecnologías informáticas y sus servicios. • Realización de acciones no autorizadas de comprobaciones de vulnerabilidades contra sistemas informáticos nacionales o extranjeros. • Introducir, ejecutar, distribuir o conservar en los medios informáticos programas que pueden ser utilizados para comprobar, monitorear o transgredir la seguridad; así como información contraria al interés social, la moral y las buenas costumbres. • Realización de administración remota de los Servidores y estaciones de trabajo empleando conexiones conmutadas. • Colocación de páginas o sitios Web desde entidades estatales en servidores extranjeros que ofrecen estos servicios de forma gratuita. • Vincular cuentas de correo electrónico de un Servidor de la entidad a Servidores en el exterior del país. • Difundir a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas o que lesione la Seguridad Nacional. • Envío de mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (SPAM). • Explorar o monitorear las redes públicas de transmisión de datos en busca de vulnerabilidades o información sobre los usuarios legales de las mismas. • Se accede sin autorización o se agrede a cualquier sistema de cómputo conectado a redes públicas de transmisión de datos y la	Art. 19 Art. 21 Art. 25 Art. 26 Art. 63 Art. 72 Art. 77 Art. 79 Art. 80 Art. 84 Art. 85			

	usurpación de los derechos de acceso de usuarios.				
1.16	¿Se tiene definido un procedimiento para la solicitud y aprobación de los usuarios de la red informática y los servicios asignados (Internet, Correo Electrónico, accesos remotos, FTP, Chat, etc)? Al menos, debe incluir: ❖ Modelo establecido para la solicitud (como mínimo debe contener el nombre y apellido del trabajador, departamento donde labora, cargo que ocupa, servicios que solicita, breve fundamentación de la solicitud, identificador que utilizará) ❖ Nivel de aprobación (firma del jefe departamento y del máximo dirigente) ❖ Definir el responsable de archivar las planillas de solicitud y períodos de vigencia.	Art. 20 y 46			
1.17	¿Se tiene elaborado un procedimiento o instrucción para autorizar y controlar el acceso a las tecnologías de información por personal ajeno a la entidad?	Art. 23			
Clasificación y control de los bienes informáticos.					
1.18	¿Existen usuarios que utilizan las tecnologías de la información en cuestiones que no son de interés de la entidad y no se corresponden con el objeto social? ❖ Uso indiscriminado del espacio de los discos duros para videos musicales, películas, juegos, novelas, música e informaciones contrarias al interés social, la moral y las buenas costumbres. ❖ Almacenamiento de programas utilizados para comprobar, monitorear o transgredir la seguridad. ❖ Realización de trabajos ajenos a sus funciones de trabajo.	Art. 12 inc c), 13 y 26			
1.19	¿Se encuentran identificados y controlados los bienes informáticos, incluyendo un inventario hasta nivel de componentes y las especificaciones técnicas de aquellos que pudieran ser suplantado y estos se encuentran	Art. 14			

	incluidos en el expediente técnico de cada medio?				
1.20	¿Los bienes informáticos se encuentran bajo la custodia documentada de una persona que responda por su protección?	Art. 15			
1.21	¿Se tiene elaborado un procedimiento para el control y autorización del movimiento de los bienes informáticos? ❖ ¿Definen los responsables de mantener actualizados los controles de los bienes informáticos? ❖ ¿Están definidos los períodos establecidos para realizar el chequeo de los bienes informáticos? ❖ ¿Existe un modelo de solicitud para realizar los traslados? ❖ ¿Quién o quienes lo autorizan? ❖ ¿Los medios informáticos existentes en el local se corresponden con el inventario del mismo? ❖ ¿Son efectivas las medidas establecidas para el control y autorización del movimiento de los bienes informáticos?	Art. 16			
1.22	¿Se controlan los soportes de almacenamiento portátiles externos (memorias flash, laptop, cámaras fotográficas, discos duros, etc.) y de la información que almacenan? • Tienen definido algún mecanismo de control (software o medidas organizativas). • Revisar los historiales de las estaciones de trabajo, para evidenciar sí los mecanismos de control son efectivos (recomendamos herramienta portable **USBDeview.exe o Evidence Collector**). • Existe constancia documental sobre las supervisiones que se realizan a estos medios.	Art. 16			
1.23	¿Se cuenta con un inventario actualizado de los sistemas informáticos y software autorizado por la dirección de la entidad? • Nombre de la aplicación y versión. • Breve descripción. • Departamento o áreas donde se utilizan. • Características principales del producto. • Suministrador de la aplicación.	Art. 10 inc) e y 16			

Gestión de Incidentes de seguridad.					
1.24	¿Tienen definida la estrategia a seguir ante la ocurrencia de incidentes o violaciones de la seguridad?	Art. 86			
1.25	¿Se establecieron las medidas y procedimientos para garantizar la continuidad, el restablecimiento y la recuperación de los procesos informáticos a partir de la estrategia definida? ❖ Medidas a ejecutar por cada tipo de incidente o violación de la seguridad. ❖ Responsables. ❖ Recursos necesarios para su ejecución. En muchos planes de seguridad informática aparece como el plan de contingencia.	Art. 87 y 88			
1.26	¿Se establecieron correctamente las medidas y procedimientos para la gestión de incidentes y violaciones de seguridad informática? Donde deben definir: ❖ Reporte inmediato de la acción a la autoridad correspondiente. ❖ La comunicación con los afectados o los involucrados en la recuperación del incidente. ❖ El análisis y la identificación de las causas del incidente. ❖ Registro de todos los eventos vinculados con el incidente. ❖ Recolección y preservación de las trazas de auditoria y otras evidencias. ❖ La planificación y la implementación de medidas para prevenir la recurrencia.	Art. 89			
1.27	¿Se tiene contemplada la designación de la comisión de investigación prevista ante la ocurrencia de incidentes? ¿Existe constancia documental sobre su funcionamiento? ❖ Sí tenemos evidencias de la ocurrencia de incidentes o violaciones de seguridad informática en la entidad controlada, podríamos emplear esta información para solicitar los resultados de las investigaciones.	Art. 90			
1.28	¿Al producirse un incidente o violación de la	Art. 91			

	seguridad informática se reporta la información oportunamente a la OSRI y a la instancia superior de la entidad? ❖ Sí tenemos información sobre la ocurrencia de hechos delictivos, incidentes o violaciones de seguridad en la entidad controlada, se pueden tomar como evidencias para demostrar que no los reportaron. Ejemplo: En coordinaciones realizadas con el MININT nos informan cuando salen incidencias en los partes sobre tecnologías informáticas (principalmente robos de computadoras y accesorios). ❖ En los análisis del servicio de correo electrónico se puede detectar el envío y/o recepción de SPAM y HOAX. Algunas de las problemáticas identificadas durante el control constituyen incidentes, tales como: ❖ Presencia de virus informáticos. ❖ Vulnerabilidades. ❖ Accesos no autorizados. De ser detectadas entonces no es efectiva la estrategia definida para la gestión de incidentes.				
Seguridad Física y Ambiental					
2.1	¿Se tienen definidas las tecnologías de información que por las funciones a que estén destinadas, la información que contengan y las condiciones de los locales requieran la aplicación específica de medidas de protección física?	Art. 27			
2.2	¿Se encuentran ubicadas las tecnologías de información en áreas que impidan su empleo para cometer acciones malintencionadas o delictivas? ❖ Comprobar el estado constructivo y de seguridad que tienen los locales (puertas, ventanas).	Art. 28			
2.3	¿Se definieron las áreas o zonas controladas en correspondencia con las denominaciones establecidas en la Resolución 127? ❖ Limitadas. ❖ Restringidas ❖ Estratégicas	Art. 29			
2.4	¿Para la selección y diseño de las áreas	Art. 31			

	controladas se consideraron las posibilidades de daño por fuego, inundación, explosión, perturbaciones del orden y otras formas de desastres naturales o artificiales?				
2.5	¿Los equipamientos informáticos ubicados en las áreas o zonas controladas se encuentran protegidos contra fallas de alimentación y otras anomalías eléctricas? ❖ ¿Existen de fuentes de alimentación ininterrumpida (UPS)? ❖ ¿Tienen sistema de aterramiento? ❖ ¿Existen identificadores de los parámetros de voltaje en las tomas de alimentación eléctrica? ❖ ¿Existen reguladores de voltaje? ❖ ¿Tienen generadores de energía alternativos (no es obligatorio en todos los casos)?	Art. 32			
2.6	¿Se cumplen las medidas previstas para las áreas limitadas? ❖ Sistemas de cierres seguros. ❖ Control del nivel de acceso. ❖ Existencia de registros para el control de las autorizaciones de trabajar fuera del horario laboral.	Art. 33			
2.7	¿Se cumplen las medidas previstas para las áreas restringidas, además de las mencionadas en el punto 2.6? ❖ Verificar que las tecnologías no estén conectadas a medios que se encuentren fueras de estas áreas o redes públicas de transmisión de datos (No pueden tener servicios de Internet). ❖ Existen sistemas de detección de intrusos y alarmas. ❖ Prohibida la introducción de soportes ópticos y magnéticos personales, excepto los autorizados por la dirección de la entidad. ❖ Prohibida la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a la misma.	Art. 34			
2.8	¿Se cumplen las medidas previstas para las	Art. 35			

	áreas estratégicas, además de las mencionadas en los puntos 2.6 y 2.7? ❖ Existencia de un registro para el control de las autorizaciones excepcionales autorizadas por la máxima dirección de la entidad.				
2.9	¿Se tiene implementado algún sistema de sellaje y/o candado de las tecnologías de la información con el objetivo de detectar y/o proteger contra alteraciones o sustracciones?	Art. 36			
2.10	¿Las tecnologías informáticas se encuentran funcionando con los chasis abiertos, facilitándose la alteración o sustracción de los componentes?	Art. 36			
2.11	¿Se encuentran dispositivos y componentes en las áreas de forma desorganizada y sin protección (MODEM, discos duros, memorias, tarjetas, monitores, unidades centrales, microprocesadores, bocinas, étc) facilitándose su sustracción?	Art. 36			
2.12	¿Se tiene limitado el arranque del sistema operativo solamente desde el disco duro y protegido con contraseña? Con esta acción se evita que puedan acceder al sistema sin restricción y realicen cualquier acción con la información (alteración, borrado o sustracción) ❖ Reiniciar la computadora e introducir un CD ROM booteable para comprobar sí podemos acceder al sistema.	Art. 36			
2.13	¿Se tiene protegida con contraseña la entrada al SETUP? Con esta acción se evita que puedan entrar personas no autorizadas y modifiquen la configuración de la máquina. ❖ Reiniciar la computadora y pulsar la tecla definida para entrar al SETUP (la visualiza en la parte inferior de la pantalla; en muchas de las computadoras se emplea DEL, F2, F8).	Art. 36			
2.14	¿Se encuentran protegidos los cables de alimentación o de comunicaciones que transportan datos contra la intercepción o el daño? ❖ Muchas de las redes son implementadas	Art. 37			

	por los propios informáticos y sin recursos, observándose cables de red o fibra óptica sin protección y otros que los transportan por cualquier lugar sin analizar los riesgos (por encima de viviendas). ¿Los cables de alimentación se encuentran separados de los cables de comunicaciones para evitar la interferencia?				
2.15	¿Los equipos informáticos se encuentran funcionando de acuerdo con las especificaciones recomendadas por los fabricantes para garantizar su disponibilidad e integridad? ❖ Apropiados controles ambientales: humedad, temperatura y protección contra el polvo.	Art. 38			
2.16	¿Se cumplen los mantenimientos de las tecnologías informáticas de acuerdo con los intervalos de servicio y especificaciones del fabricante? ❖ ¿Existe contrato de mantenimiento? ❖ ¿Se registran y controlan los mantenimientos realizados? ❖ ¿Se cumplen los períodos establecidos para realizar los mantenimientos? ❖ ¿Las computadoras e impresoras se encuentran en buenas condiciones y los niveles de polvos son bajos?	Art. 38			
2.17	¿Existe un procedimiento para autorizar el empleo de las tecnologías informáticas fuera de las instalaciones de la entidad? ❖ ¿Tienen establecido un modelo de solicitud para realizar los traslados de las tecnologías informáticas y emplearlas fuera de las instalaciones de la entidad? ❖ ¿Definen los motivos del traslado del medio y en qué funciones se empleará? ❖ ¿Se registran los datos generales del trabajador que realiza la solicitud y de la persona que autoriza? ❖ ¿Se definen las responsabilidades y obligaciones que deben cumplir para garantizar la protección del medio y de la información? ❖ ¿Definen los responsables de archivar los	Art. 39			

	modelos de solicitud y aprobación? ❖ ¿Está instrumentada la revisión de las tecnologías informáticas cuando son retornadas a la entidad y quienes son los responsables de su realización.				
2.18	¿Cuentan con un procedimiento adecuado para evitar que la información contenida en los equipos, que causen bajas o sean destinados para otras funciones, pueda resultar comprometida? ❖ ¿Tienen definidas las medidas y acciones a realizar para los dispositivos de almacenamineto que tienen informaciones críticas y sensibles. ❖ ¿Está definido el método a emplear para la destrucción de la información y ante qué situaciones? ❖ ¿Se definen los responsables de ejecutar y controlar el proceso de destrucción de la información? ❖ Solicitar los documentos sobre las bajas de las tecnologías informáticas y verificar sí cumplieron con el procedimiento.	Art. 40			
2.19	¿Se registran a la entrada y salida de la entidad los traslados de equipos, información o software donde quede constancia del documento oficial que demuestre su legalidad? ❖ Verificar si existe en la entrada principal de la instalación un registro de control para estos fines.	Art. 41			
2.20	¿Se tiene definido un procedimiento para el control de los usuarios que emplean las tecnologías informáticas y sus servicios en instalaciones de acceso público? Nos referimos a Ciber Café de los Hoteles, salas de navegación de Correos de Cuba, Bibliotecas, Joven Club de Computación, Laboratorios de computación, etc. ❖ ¿Está definido un mecanismo de control para registrar el acceso a las instalaciones? ❖ ¿Se registran los datos generales de las personas que acceden (nombre y apellido,	Art. 4 Art. 27			

	carné de identidad) y otras informaciones importantes para una investigación como son: Fecha y hora de entrada, Fecha y hora de salida, equipo informático empleado, nombre del área donde se encontraba trabajando)? ❖ ¿Se encuentra establecido el período de vigencia de archivar los registros? ❖ ¿Están definidas las responsabilidades de las personas que deben garantizar la regulación del control de acceso? ❖ ¿Existen evidencias sobre la realziación de supervisiones a los locales de forma sistemática y sorpresiva? ❖ ¿Existen registros de incidencias? ❖ ¿Tienen definido un método de identificación y autenticación para acceder a las tecnologías informáticas y los servicios (tarjetas magnéticas, login y password)?	Art. 45 y 69			
Seguridad en el control de acceso					
Identificación, autenticación y control de accesos.					
3.1	¿Se tienen definidos los identificadores de usuarios de forma personal y única? ❖ Verificar las cuentas de usuarios que están creadas en las computadoras. ❖ Comprobar la relación existente entre la cantidad de usuarios que emplean la computadora y la cantidad de cuentas. ❖ Comprobar sí la persona que estaba trabajando en el momento de la revisión, estaba utilizando su identificador o de otra persona. **En LINUX**: El fichero que contiene las cuentas creadas se encuentra en el directorio ***/etc*** y el fichero se identifica como **passwd** y el fichero **shadow** contiene las cuentas con sus contraseñas encriptadas. En la consola correr el comando siguiente: $ **finger** julio (suponiendo que julio está dentro del fichero paswd o probar alguna cuenta que obtuvimos en informaciones anteriores)	Art. 45			

	Sí tienen habilitado ese servicio (**finger**) y mal configurado nos posibilitará obtener informaciones valiosas para la inspección o buscar vulnerabilidades al sistema.				
3.2	¿Se tiene establecido un procedimiento para la eliminación de los identificadores de usuarios, ya sea por cesar sus relaciones laborales u otras causas? 5.5 El departamento de recursos humanos tiene instrumentado informar al administrador de la red; sobre las bajas, certificados y licencias de los trabajadores con el objetivo de eliminar o deshabilitar temporalmente las cuentas. 5.6 Obtener en recursos humanos la relación general de los trabajadores y de los que presentan limitaciones de trabajar. (En ocasiones se ha solicitado la última nómina) Chequear esta información con la existente en el Servidor e identificar posibles violaciones al respecto. 5.7 De existir violaciones, se toman como evidencias para incorporarlas en los anexos del informe.	Art. 46			
3.3	¿Se tienen definidas las directivas de seguridad para las contraseñas y las cuentas? Qué garanticen: ❖ ¿Se obliga el empleo del nombre de usuario y contraseña? ❖ ¿No se visualiza el nombre de usuario de la anterior conexión? ❖ ¿Se obliga a cambiar la contraseña en correspondencia con el período definido en el PSI? ❖ ¿Se almacenan las contraseñas para evitar que se repitan? ❖ ¿Tienen definidos los requerimientos de seguridad para las contraseñas, estableciendo que sean alfanuméricas y con una longitud no menor de seis caracteres? ❖ ¿Se bloquea el usuario que sea incapaz de	Art. 47 inc b) inc b) inc b) y c)			

	introducir correctamente la contraseña, después de un número determinado de intentos erróneos? (se recomienda como máximo cinco intentos) **En LINUX**: La creación de las cuentas con el commando **useradd** coge por defecto los parámetros definidos en el fichero **/etc/login.defs**				
3.4	¿Los usuarios hacen uso de sus respectivos login/password y no utilizan otros?	Art. 47 inc a)			
3.5	¿Se tiene habilitada la opción de recordar la contraseña para acceder a los servicios (correo electrónico, conexión conmutada, Internet, Chat, FTP, SSH, conexiones remotas, étc)?	Art. 47 inc a)			
3.6	¿Se visualizan las contraseñas mientras se teclean?	Art. 47 inc d)			
3.7	¿Se encuentran almacenadas en texto claro (sin cifrar) las contraseñas, ya sea en las tablas de las bases de datos o en archivos? ❖ En las bases de datos acces y SQL existen tablas para definir los usuarios y sus contraseñas, sin embargo en las propiedades del campo lo ponen como texto y no como contraseña. Entonces posibilita que puedan obtenerse las contraseñas fácilmente. ❖ Realizar búsquedas en las estaciones de trabajo (hemos tenido efectividad poniendo como criterio de búsqueda las palabras: clave, claves, contraseña, password, pw, seguridad, acceso). Aunque parezca ingenuo este método, podríamos asegurar su efectividad en muchas de las entidades controladas, porque se han detectado documentos y correos contentivos de esas informaciones.	Art. 47 inc e)			
	¿Se tienen definidos los requisitos y procedimientos de seguridad para proteger el equipamiento que dejan desatendido por un período de tiempo, así como de su responsabilidad de implementar tal protección?	Art. 45 y 48			

	❖ ¿Se encuentran sesiones de trabajos activas por tiempos prolongados, donde el usuario no se encuentra presente en el local? ❖ ¿Se tienen habilitados los protectores de pantalla protegidos con contraseñas, ante un tiempo determinado de inactividad? ❖ ¿Se apagan los monitores de las estaciones de trabajo y Servidores; sin embargo existen sesiones abiertas referentes a servicios (Internet, Chat, correo) o accesos a informaciones y sistemas?				
Derechos y privilegios de acceso a sistemas y datos.					
3.8	¿Tienen definido un procedimiento escrito para otorgar o suspender los derechos y privilegios de acceso a sistemas y datos? Al menos, debe incluir: ❖ ¿Está definido el modelo de solicitud? ❖ ¿Se establece a qué sistema informático tendrá acceso el usuario, definiendo sus roles para acceder a los diferentes módulos de la aplicación? Ejemplo: Sistema informático SISCONT 5 Módulos de acceso: Cobros y pagos, facturación. ❖ ¿Se corresponde el nivel de aprobación (firma del jefe departamento y del máximo dirigente)? ❖ ¿Está definido el responsable de archivar las planillas de solicitud y de comprobar su cumplimiento?	Art. 48			
3.9	¿Se encuentran definidos y restringidos correctamente los derechos de accesos y permisos de los usuarios sobre los directorios sensibles de los sistemas? (Ejemplo: C:\Winnt y sus interiores) En plataforma Windows verificar los permisos del grupo "**Todos**" y los de "**Control Total**". **En LINUX**: La primera línea de defensa es la protección del directorio **/etc/password** y **/etc/shadow**; por lo que debe verificarse sus permisos, derechos y	Art. 48			

	que no se encuentren en otras ubicaciones accesibles para usuarios no autorizados. El archivo **/etc/group** permite controlar el acceso a los archivos. Si el usuario no es el dueño del archivo, entonces se verifica sí el usuario es miembro del grupo que posee el archivo.				
3.10	¿Los recursos compartidos se realizan empleando mecanismos de identificación y autenticación para los usuarios o grupos que tienen acceso autorizado a los mismos? ❖ Buscar los recursos compartidos en la red. ❖ Intentar conectarnos a los recursos compartidos con el objetivo de determinar aquellos que no tienen mecanismos de identificación y autenticación. ❖ A los recursos compartidos que permitieron conectarnos, debemos revisar sus permisos y derechos. Sí algunos de estos, coinciden con los bienes informáticos de mayor importancia definidos en el análisis de riesgos o que contengan informaciones sensibles, bases de datos o aplicaciones críticas se procederá a tomar las evidencias de las acciones realizadas para anexarlas al informe.	Art. 48			
3.11	¿El Administrador de la red tiene otra cuenta, como un usuario normal para su desempeño, que no se relacione con las actividades propias de la administración?	Art. 48			
3.13	¿Existen usuarios que han sido trasladados de área de trabajo y aún poseen derechos que no se corresponden con su nueva función? ❖ Verificar las cuentas de administración y el grupo de administradores del dominio. Hemos detectado, como algunos informáticos o administradores de redes se ubican en otros cargos y se mantienen sus cuentas de usuarios dentro del grupo de administradores. ❖ Verificar las cuentas creadas en los sistemas informáticos y determinar a quienes pertenecen, así como sus cargos actuales.	Art. 48			

	Se mantienen usuarios habilitados en los sistemas informáticos financieros – contables, sin embargo ya no trabajan en el área económica e incluso se han detectado algunos casos donde los propietarios de las cuentas ya no laboran en la entidad.				
3.14	¿Se encuentran en directorios diferentes los datos y las aplicaciones, para facilitar la limitación de los accesos? ❖ Comprobar las ubicaciones de las aplicaciones y datos. ❖ De existir en el mismo lugar, deben chequearse los permisos y derechos, y si tienen habilitadas las opciones de auditoria a esos directorios.	Art. 48			
3.15	¿Se tiene una correcta configuración del fichero **adduser.conf** para la creación de los usuarios del sistema en los Servidores con sistema operativo LINUX? ❖ Obtener el fichero password del Servidor que se encuentra ubicado en **\etc** y comprobar los shell de comandos asignados a las cuentas de usuarios. Ejemplo: root:x:0:0:root:/root:/**bin/bash** jose:x:1000:1000:Jose:/home/jose:**/bin/bash** test:x:1002:1002:test Mio:/home/test:**/bin/bash** Aquí se aprecia que todas las cuentas tienen **/bin/bash** (shell de comandos con privilegios) y esto constituye una vulnerabilidad que puede ser aprovechada por un atacante. Revisar la configuración del fichero **adduser.conf**, porque cuando se instala LINUX el trae por defecto la asignación de **/bin/bash** a todas las cuentas. Se recomienda ponerle **/bin/false** o **/sbin/nologin**	Art. 48			
Seguridad de Operaciones.					
4.1	¿Se tuvo en cuenta el principio de separación de	Art. 42			

	funciones (tareas que no debe realizar una misma persona) al determinar las responsabilidades asignadas al personal considerando aquellas que no deben ser realizadas por una misma persona? ❖ Administrador de red. ❖ Jefe Departamento Informática. ❖ Desarrollador de aplicaciones e informáticos. ❖ Especialista de seguridad informática. ❖ Jefe Departamento Económico.				
4.2	¿Se tiene confeccionado un manual de procedimiento que establezca y regule el empleo de los sistemas informáticos, definiéndose las obligaciones y responsabilidades teniendo en cuenta el principio de separación de funciones?	Art. 42			
4.3	¿Los sistemas informáticos financieros - contables y la base de datos que brinda soporte a la aplicación, se encuentran instalados en la misma computadora y también se emplea como una estación de trabajo? ❖ Este riesgo incrementa la posibilidad de modificación no autorizada de la información (intencional o por error).	Art. 42			
4.4	¿Se tienen definidas diferentes cuentas con privilegios de administración y no se justifica su creación, dificultándose la delimitación de responsabilidades ante la ocurrencia de cualquier incidente de seguridad o durante un proceso de investigación? ❖ Verificar el grupo de **Administradores del dominio** e identificar las cuentas que pertenecen a este y analizar cada caso para definir su propietario y el cargo que ocupan. ❖ Determinar la cantidad de cuentas que tienen privilegios de administración local del equipo. ❖ Verificar en las aplicaciones informáticas las cuentas creadas y determinar las que tienen habilitados sus roles de administración. Resulta común, encontrarnos que todas las cuentas creadas en las aplicaciones tienen privilegios de administración, permitiéndoles a	Art. 42			

	personas no autorizadas la posibilidad de crear usuarios, modificar roles de accesos a los módulos y borrar los historiales del sistema.				
4.5	¿Se tiene definido un procedimiento para regular y aprobar la introducción de nuevos sistemas informáticos, actualizaciones y nuevas versiones en correspondencia con el sistema de seguridad?	Art. 43			
4.6	¿Los Softwares instalados se corresponden con los autorizados por la dirección de la entidad? ❖ Buscar todos los Softwares instalados. ❖ Comprobar, sí los Softwares instalados se encuentran dentro del inventario de los sistemas informáticos y aplicaciones autorizadas. ❖ Guardar las evidencias sobre los Softwares no autorizados, registrándose el nombre del producto, camino de ubicación del programa instalado y fecha de instalación. ❖ Determinar, para qué se emplean los softwares no autorizados detectados e identificar aquellos que violan alguna de las políticas de seguridad definidas para la entidad o constituyen violaciones de la Resolución 127. (Proxys anónimos, borrado de historiales, programas para encriptación de datos y particiones completas de discos duros, escaneadores de vulnerabilidades, étc)	Art. 10 e) y 43			
4.7	¿Se tiene definido un procedimiento para controlar las acciones realizadas con vista a cubrir las brechas de seguridad y la corrección de los errores del sistema? Deben asegurar: ❖ ¿Están definidas las personas autorizadas para acceder a los sistemas en funcionamiento y datos? ❖ ¿Las acciones de emergencia tomadas son documentadas? ❖ ¿Se informan a la máxima dirección?	Art. 44			
4.8	¿Existe una política de actualización de los Sistemas Operativos de los Servidores y de los softwares instalados en los mismos en cuanto a brechas de seguridad detectadas y publicadas en sitios de seguridad en Internet?	Art. 44			

4.9	¿Se emplean cuotas en los discos duros para realizar la gestión eficiente del espacio compartido por múltiples usuarios?	Art. 42 y 44			
4.10	Se documentan los mantenimientos preventivos a las computadoras y correcciones de los sistemas, tales como: ❖ Borrado de ficheros temporales. ❖ Desfragmentación de los discos duros. ❖ Reinstalación del sistema operativo. ❖ Reinstalación o correcciones de las aplicaciones informáticas y bases de datos.	Art. 44 inc b)			
Seguridad ante programas malignos.					
4.11	¿Se aplican medidas que evitan el diseño, distribución o intercambio de códigos de virus informáticos u otros programas malignos entre personas naturales o jurídicas?	Art. 49			
4.12	¿Tienen implementados los controles y procedimientos para protegerse contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para impedir su generalización?	Art. 50			
4.13	¿Se tiene definida una política de seguridad que regule la descarga de archivos y softwares desde redes externas o cualquier otro medio, indicando las medidas de seguridad que deben ser adoptarse antes de instalarse o correrse cualquier fichero adquirido?	Art. 50			
4.14	¿Se tienen definidos los programas antivirus y se encuentran actualizados? ❖ ¿Cúal o cúales antivirus utilizan? ❖ ¿Cómo tienen configurada su actualización? ❖ ¿La forma de obtener las actualizaciones garantiza su actualización diaria? ❖ ¿Los usuarios saben cómo actualizar los antivirus y lo realizan sistemáticamente? El empleo de dos o más productos de software antivirus, puede mejorar la eficacia y niveles de detección de los virus informáticos. (Por lo tanto, no lo considero como una deficiencia)	Art. 50			
4.14	**¿Se tiene como directiva de seguridad la desactivación del arranque automático de todas las unidades o dispositivos para evitar la propagación de virus?**	**Art. 50**			

	➢ **Introducir una memoria flash y comprobar que no permite su arranque automático.**				
4.15	¿Se cumplen los procedimientos establecidos ante indicios de contaminación por programas malignos, tanto en redes como en equipos no conectados a redes? Sí detectamos virus informáticos en la red, entonces no cumplen con el procedimiento que es proceder al cese de las operaciones de los medios contaminados y a su desconexión de las redes, preservándolos para su posterior análisis y descontaminación.	Art. 51			
4.16	¿La contaminación por virus informáticos u otros programas malignos los tienen considerados como un incidente de seguridad? ❖ ¿En el PSI lo tienen contemplado como un incidente de seguridad? ❖ ¿Tienen definido informar a la OSRI e instancias superiores?	Art. 52			
Respaldo de la información.					
4.17	¿Se emplean procesos de tolerancias a fallos en los Servidores mediante el empleo de arreglos de discos o Server espejos? ❖ Verificar sí realmente utilizan Servidores profesionales o computadoras configuradas como Servidores. ❖ Los servidores profesionales tienen arreglos de discos (RAID). ❖ Se cuentan con servidores espejos que garantizan la réplica de las informaciones y servicios.	Art. 53			
4.18	¿Se tiene definido un procedimiento para realizar las copias de seguridad? ❖ ¿Tienen definidas las informaciones a salvar? ❖ ¿Se definen los medios y ubicaciones donde se salvaran las informaciones? ❖ ¿Se definen específicamente las responsabilidades de las personas que deben garantizar las salvas y su seguridad?	Art. 53			

	❖ ¿Tienen establecida la periodicidad de las salvas y se corresponde con la importancia de la información? ❖ ¿Se establece una forma de notificación o registro documental que evidencie la realización de las salvas y su estado? ❖ ¿Tienen contemplado el almacenamiento de otra salva en otra ubicación?				
4.19	¿Se realizan las salvas con la periodicidad definida y verifican su realización? ❖ Comprobar la existencia de las salvas. ❖ Chequear las propiedades de las salvas para definir la fecha de realización y comprobar su correspondencia con la periodicidad definida. ❖ Comprobar si existen constancias documentales sobre la realización de supervisiones a los medios de salvas, su estado técnico y contenido.	Art. 53 y 56			
4.20	¿Los usuarios realizan según el período definido las salvas de la información que se vinculan con sus funciones? ❖ Comprobar si tienen definidos espacios de discos duros en los Servidores u otras ubicaciones para realizar las salvas de informaciones de los usuarios. ❖ Verificar sí los usuarios realizan las salvas periódicamente y los tipos de informaciones.	Art. 53			
4.21	¿Se dispone de dispositivos externos y equipos informáticos para la ejecución de copias de seguridad en la red? ❖ Comprobar si existen discos duros externos, DVD, CD y otros medios que garanticen salvas externas. ❖ Verificar si existen salvas cruzadas entre servidores o estaciones de trabajo.	Art. 53			
4.22	¿Existen copias de las configuraciones de los servidores, instaladores de aplicaciones, sistemas operativos y sistemas financieros - contables? ❖ Comprobar sí las salvas realizadas contienen las configuraciones de los Servidores, instaladores de sistemas y aplicaciones.	Art. 53			

4.23	¿Se tiene una información de respaldo de conjunto con los informes de las copias y el procedimiento de recuperación en otra ubicación fuera de la entidad? ❖ ¿Existe constancia escrita de su traslado y recepción? ❖ ¿Verificar su existencia y condiciones de almacenamiento? ❖ ¿Comprobar las propiedades de las salvas para concocer su fecha de realización y su estado técnico?	Art. 54			
4.24	¿Se emplean cuotas de disco para realizar la gestión eficiente del espacio compartido en disco por múltiples usuarios?	Art. 54			
4.25	¿Se mantienen las informaciones almacenadas en lugares seguros y que cumplan con los requisitos ambientales?	Art. 55			
Seguridad de las Redes y sus servicios					
5.1	¿Se tiene un inventario actualizado de los dispositivos y medios existentes en el local de los Servidores? 5. Comprobar si tienen control e inventario de los medios existentes en el local de los servidores (MODEM, HUB, Switch, Router, Servidores, terminales, líneas telefónicas, puntos de accesos inalámbricos, PLC, y todo equipo relacionado con las comunicaciones). 6. Verificar sí los medios existentes se encuentran inventariados y pertenecen a la entidad.	Art. 10 inc e)			
5.2	¿Se cumple con las restricciones de los niveles de accesos al local de los Servidores? ❖ Comprobar si existen otras personas dentro de las áreas que no pertenecen a éstas u otro personal ajeno a la entidad. ❖ Tomar imágenes sobre los niveles de accesos y posibles violaciones graves que se cometen en este sentido (puede ser anexada al informe). ❖ Verificar sí existen fotos o videos tomadas en locales de áreas restringidas y	Art. 33, 34 y 35			

	estratégicas. En controles nos hemos encontrado en los discos duros la presencia de fotos y videos filmados en los locales de Servidores, elementos que nos sirven como evidencias de esas violaciones.				
5.3	¿El local de los servidores se encuentra compartido con otras áreas no vinculadas a la actividad informática? Comprobar sí: ❖ Se encuentran ubicados los servidores en el departamento de economía u otras áreas. ❖ Para acceder a otros departamentos se necesita circular por el local de los Servidores, no existiendo delimitación entre ambos.	Art. 33, 34 y 35			
5.4	¿Se tiene establecida una política de seguridad y medios de control para establecer los servicios autorizados, protocolos, puertos y reglas de accesos implementadas para garantizar que se bloqueen los no autorizados? ❖ ¿Se definen claramente los servicios autorizados en la entidad y los puertos a utilizar? ❖ ¿Se tienen establecidas las medidas de seguridad y de control para garantizar la seguridad de los servicios? ❖ ¿Definen las responsabilidades de las personas encargadas de garantizar la implementación de las medidas de seguridad y su supervisión?	Art. 57			
5.5	¿Las informaciones sensibles y clasificadas solamente son accedidas desde las estaciones de trabajo debidamente autorizadas y son impresas solamente en las impresoras compartidas para tales efectos?	Art. 57			
5.6	¿Existe una política de seguridad en cuanto a compartir recursos en la red? Comprobar sí:	Art. 57			

	❖ Los recursos se comparten mediante contraseñas o de sólo Lectura, o ambas. ❖ No se comparten totalmente los discos duros. ❖ No se comparten directorios sensibles del sistema. ❖ No se comparten directorios o carpetas que contengan programas y/o bases de datos sensibles. En LINUX para compartir recursos se emplea comúnmente SAMBA y su fichero de configuración se encuentra en el fichero **/etc/samba/smb.conf**. **Parámetro workgroup.** Se establece el grupo de trabajo, ejemplo: workgroup = OSRI-HLG **Parámetro hosts allow.** Puede emplearse para establecer la lista de control de acceso que definirá las máquinas o redes autorizadas a acceder hacia el servidor. **Parámetro interfaces.** Permite establecer desde que interfaces de red del sistema se escucharán peticiones. Esto es útil cuando Samba se ejecuta en un servidor que sirve también de puerta de enlace para la red local, impidiendo se establezcan conexiones desde fuera de la red local. interfaces = lo eth0 192.168.1.254/24 **Parámetro hide dot files.** Los usuarios no deben tener acceso a ficheros ocultos del sistema, es decir ficheros cuyo nombre comienza con un punto, particularmente si acceden a su directorio personal en el servidor Samba (Ejemplo: .bashrc, .bash_profile, .bash_history, etc.). Es empleado el parámetro para complementar la configuración de los directorios personales de los usuarios. [homes]				

	comment = Home Directories browseable = no writable = yes **hide dot files = Yes** También se puede emplear el parámetro **veto files** que permite denegar el acceso a los ficheros cuyos nombres contengan las cadenas definidas. Ejemplo: [homes] comment = Home Directories browseable = no writable = yes hide dot files = Yes **veto files = /*Security*/*.tmp/** Se deniega el acceso hacia los ficheros cuyos nombres que incluyen la palabra «Security» y los que tengan extensión o terminen en «.tmp».				
5.7	¿Se tienen definidos grupos o unidades organizativas para organizar la red en correspondencia con la estructura de la entidad? Verificar sí: ❖ ¿Todos los usuarios creados están autorizados? ❖ ¿Se aplican directivas de acceso a determinados usuarios o estaciones de trabajo? ❖ ¿Existen restricciones de acceso para determinados días y horarios? ❖ ¿Se encuentra deshabilitada la cuenta de Invitado?	Art. 58			
5.8	¿Se tienen implementas las políticas de auditoria locales y a nivel de dominio adecuadas, que permita monitorear los principales eventos del sistema operativo por un tiempo no menor de un año sin afectarse el desempeño del mismo? • ¿Están determinadas las computadoras donde se configurará la auditoria? • ¿Están determinados los eventos a auditar?	Art. 58 y 62 inc a)			

	En sistemas operativos Windows existen tres registros que vienen de forma predeterminada (Aplicación, Sistema y Seguridad). Los otros tres (Servicio de Directorio, Replicación de Archivos y Servidor DNS) estarán presentes cuando se encuentran instalados los servicios apropiados. Es preciso revisar la configuración de cada registro en términos de su tamaño máximo y lo que debería ocurrir cuando alcance éste tamaño; porque por defecto viene con **512 Kbyte y sobre escritura a los siete días**. (Inicio-Herramientas administrativas- Event Viewer-click derecho y propiedades) **En LINUX**: Comprobar la configuración del fichero del Servidor que se encuentra ubicado en **/etc/syslog.conf**, porque muchos administradores tienen comentariadas la salva de los eventos y no garantizan el almacenamiento de estas trazas. Existe un archivo del sistema (syslog), un archivo de trazas para los mensajes de informaciones generales del sistema (**messages**), uno para los eventos de seguridad (**secure**), uno para el contenido de los servicios desde iniciar el sistema (**boot.log**) y un archivo para las tareas cron. Por defecto, viene para mantenerse las trazas durante cuatro semanas e identificándolos por cada una de estas. Siendo recomendable comprobar la configuración del archivo de **/etc/logrotate.conf y los** archivos de configuración en el directorio **/etc/logrotate.d** Los archivos **/var/log/wtmp** y **/var/run/utmp** contienen un registro de todos los accesos de los usuarios al sistema y deben tener permisos 644. Para nuestro trabajo, también es importante conocer que para los directorios home de cada usuario se crea un fichero **bash_history** que guarda los comandos y acciones realizadas por estos.				

5.9	¿Se tiene implementada una política de seguridad para garantizar la protección de los registros de eventos? Consideramos que debe incluir: • Definir una directiva para el almacenamiento, la sobre escritura y el mantenimiento de todos los registros de sucesos. • Delimitar los derechos y permisos de acceso a los registros de sucesos. • Habilitarse la auditoria de los aciertos y errores de los sucesos del sistema, para determinar si se producen intentos de eliminación del contenido del registro de seguridad. • Un proceso de almacenamiento periódico de los registros de sucesos en una ubicación independiente del servidor.	Art. 58			
5.10	¿Se garantiza el almacenamiento de las trazas correspondientes a los servicios habilitados por un tiempo no menor de un año? En **Windows** son importantes los registros creados por las aplicaciones DHCP (asignación dinámica de IP), RAS (accesos conmutados), ISA Server, Servicios de Internet Information Server (IIS), PROXY, WEB, Servidor de Correo Electrónico y Cortafuegos, entre otros. En **LINUX** las trazas de los servicios mencionados anteriormente se ubican en el directorio **\var\log**; no obstante es recomendable analizar los ficheros de configuración de los servicios habilitados que se encuentran en el directorio **\etc** porque pueden haberlos modificados las personas que lo instalaron. **Ejemplo: \etc\squid\squid.conf** Resulta importante revisar también la rotación de los ficheros de trazas, en la configuración ubicada en **/etc/logrotate.d/**; porque de no hacerlo correctamente permiten la sobre escritura de éstos.	Art. 58			
5.11	¿Se revisan periódicamente las opciones y	Art. 58			

	directivas de seguridad en las estaciones de trabajo que tienen MODEM, para impedir accesos no autorizados a la red? ❖ Conexiones alternativas de correo electrónico e Internet. ❖ Siempre es recomendable correr los comandos para conocer la configuración de los dispositivos de red (ipconfig/all para Windows, ifconfig para LINUX) y poder determinar si existe alguna configuración para Modem.				
5.12	¿El diseño y arquitectura de la red está acorde con el diagrama e inscripción de la red aprobada para su empleo? ❖ Realizar diseño del diagrama de la red y obtener los datos técnicos de los dispositivos utilizados (hub, switch, router, modem, modem-router, puntos de accesos inalámbricos, étc). ❖ Buscar en los historiales de los dispositivos y eventos del sistema operativo la posible utilización de otros medios. ❖ Detectar computadoras con más de una tarjeta de red y obtener sus configuraciones (ipconfig/all para Windows, ifconfig para LINUX), identificándose las IP asignadas a cada interfaz. En ocasiones se han detectado computadoras con dos tarjetas de red y una de ellas con una Ip real (**200.55.X.X**) ❖ Verificar sí existen tareas programadas por los administradores para fines personales, como por ejemplo arrancar servicios a una hora determinada, eliminar trazas, realizar determinado filtro, ejecutar un comando, etc. En plataforma LINUX debemos revisar en la ubicación **/etc/crontab** las configuraciones de las tareas programadas. Los usuarios que no son **root**, pueden configurar tareas programadas con la utilidad crontab y se almacenan en el directorio **/var/spool/cron** y se ejecutan	Art. 60			

	utilizando los nombres de los usuarios que los han creado (**/var/spool/cron/username**)				
5.13	¿Los servicios implementados en la red son los autorizados y se corresponden con las políticas definidas? ❖ Verificar las configuraciones de los Servidores y las estaciones de trabajo, sus archivos de configuración y servicios habilitados. **En plataforma Windows**: ❖ Conocer las configuraciones de la red (**ipconfig/all**). ❖ Utilizar el administrador de tarea o herramientas del portable que permitan listar los procesos, su ubicación y ejecutables relacionados con estos. ❖ Utilizar herramienta del portable o la consola de administración de equipo para verificar los servicios habilitados y su forma de ejecución (manual o automática). ❖ Conocer las conexiones establecidas, puertos y direcciones IP de las máquinas (**netstat –an**) **En plataforma LINUX** (en la consola de comandos): ❖ Conocer los parámetros de las interfaces y la información de las mismas (**ifconfig** y **ifconfig –a -s**). ❖ Verificar los encaminamientos (**route –n**) para conocer si existe conectividad a otras redes. Los ficheros se generan en el directorio **/etc/sysconfig/network-scripts/ route-eth0**, en este caso para la interfaz **eth0** ❖ Listar los procesos que están corriendo (**ps aux| less**). Por defecto todos los servicios vienen deshabilitados, para saber cúales está instalados y que están corriendo se	Art. 60			

	pueden buscar en la ubicación **/etc/init.d/**. Es importante esta información, porque algunos administradores tienen servicios que se inician por una tarea programada o lo ejecutan cuando deseen y allí apareceran los determinados demonios para cada servicios y el puerto que utilizan; por ejemplo para SSH se encontrará **/etc/init.d/sshd** En algunas distribuciones se encuentra en la ubicación **/etc/rc.d** y para el ejemplo anterior sería **/etc/rc.sshd** También, pueden utilizar **xinetd** y entonces debemos revisar la configuración del fichero **/etc/xinetd.conf** y el directorio **/etc/xinetd.d** El listado de todos los servicios que soporta la distribución LINUX, se encontrará en la ubicación **/etc/services** donde aparece el puerto que utilizan, pero para utilizarse deben ser habilitados. Por lo inseguros que son los servicios **rlogin** y **rsh** se recomienda inhabilitarlos. Además, revisar en el directorio **/etc/hosts.equiv** para comprobar sí están definiendo algunas estaciones de trabajo como confiables que permitan los servicios de mayor riesgo como son: rlogin, rcp, rcmd y rsh. Es decir, los usuarios definidos en las estaciones de trabajo definidas en **hosts.equiv** pueden acceder en los Servidores sin una contraseña. Existe otro fichero a revisar **.rhosts**, que permite además acceder al sistema con cualquiera de los usuarios definidos en **/etc/passwd**.				

	❖ Conocer las conexiones de red, encaminamiento y estadísticas de las interfaces (**netstat –puta**). También puede usar (**netstat –tupn**) que nos dará el protocolo (tcp, udp), nombre del programa y proceso, dirección IP, número de puerto y estado de la conexión. **netstat –r** (también te permite listar la tabla de ruta) Con el comando (**netstat –i**) se obtienen estadísticas sobre las interfaces de redes existentes. ❖ Supervisar la tabla de asignaciones de direcciones IP y direcciones MAC (**arp –n**) ❖ Información sobre los usuarios que están usando el sistema (**Who**) ❖ Información sobre los últimos usuarios que han utilizado el sistema (**Last**) **Atención**: Es necesario prestar atención que corriendo los comandos **ipconfig** o **ifconfig**, pueden aparecer otras configuraciones que nos evidencian configuraciones sobre virtualización de sistemas operativos. Tanto en LINUX como en Windows, aparecen las interfaces de las redes virtuales. En **Windows** también lo observamos cuando seleccionamos ver todas las configuraciones de las redes y se crea la carpeta **My Virtual Machines** en la ubicación **C:\Documents and Settings\Administrador\Mis documentos**. En LINUX se encontrará en el directorio **/home/** del usuario que instaló la máquina virtual y el nombre del directorio dependerá del programa empleado para virtualizar.				
5.14	¿Se tiene designada una persona para la Administración de la red?	Art. 61			
5.15	¿El administrador de la red tiene conocimiento sobre las obligaciones que tiene en relación a la	Art. 62			

	seguridad informática?				
5.16	¿Se tienen instaladas las herramientas necesarias para analizar los eventos generados por el sistema operativo y los servicios que brindan?	Art. 62 inc b) y c)			
5.17	¿Se tienen en cuenta los análisis de las trazas para evaluar la calidad de los servicios y se alerta a la máxima dirección sobre su mal uso, posibles ilegalidades o intrusiones al sistema?	Art. 62 inc d)			
5.18	¿El Administrador de la red no activa los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando la información requerida para su esclarecimiento?	Art. 62 inc h)			
5.19	¿Tienen elaborado un procedimiento donde establezcan oficialmente las responsabilidades, obligaciones y puestos de trabajos desde donde pueden realizar las tareas de administración remota de los Servidores y estaciones de trabajo? ❖ ¿Está definido quién o quienes pueden realizar las tareas de administración remota? ❖ ¿Están definidos los puestos de trabajo desde donde se realizaran las tareas de administración remota? ❖ ¿Se tienen guardadas las trazas de estos eventos?	Art. 63			
5.20	¿Se realizan acciones de administración remota de los Servidores y estaciones de trabajo **empleando conexiones conmutadas**? ❖ ¿Las cuentas de administrador, administrador del dominio y root tienen la posibilidad de conectarse de forma remota por el servicio RAS? ❖ Analizar las trazas del servicio RAS e identificar si existen conexiones con las cuentas de administración. ❖ Analizar los eventos del sistema operativo para determinar las conexiones realizadas con las cuentas administrativas y las direcciones IP desde donde se realizaron las conexiones; con el objetivo de evidenciar las correspondientes a	Art. 63			

	conexiones conmutadas. Recordar que esto es una prohibición y una violación GRAVE.				
5.21	¿Se tiene regulado el uso de las cuentas de administración, solamente para acciones que necesiten el máximo de privilegios y ejecutar tareas concretas? ❖ Analizar los eventos de los sistemas para evidenciar el uso indiscriminado de las cuentas de administración.	Art. 63			
5.22	¿En las políticas de seguridad se prohíbe la adición de algún equipo o la introducción de cualquier tipo de software en la red, sin la autorización de la entidad?	Art. 64			
5.23	¿Se permiten conexiones desde o hacia el exterior, sin existir los medios técnicos y lógicos que aseguren una barrera de protección entre las tecnologías de información de la entidad y la red externa? ❖ ¿Tienen configurados cortafuegos, sistemas de detección de intrusos (IDS)? ❖ ¿Se tienen definidas las reglas de accesos?	Art. 66			
5.24	¿Las configuraciones de los cortafuegos y sistemas de detección de intrusos (IDS) tienen habilitadas las opciones de seguridad y reglas de accesos que garanticen la barrera de protección? ❖ ¿Las reglas de acceso implementadas en la práctica se corresponden con el análisis de riesgo y son efectivas? ❖ ¿Se guardan las trazas de las conexiones? ❖ ¿Se analizan los eventos generados por el cortafuego o IDS? **En plataforma LINUX**: En las entidades emplean principalmente como cortafuegos **Iptables** o **Shorewall**. En el caso de visualizar las reglas definidas para	Art. 66			

	el primero se emplea el comando **iptables –nL**. Esta información se encuentra en el fichero **/etc/sysconfig/iptables.** Cuando no hay reglas ni cadenas cargadas, la salida debe devolver lo siguiente: Chain INPUT (policy ACCEPT) target prot opt source destination Chain FORWARD (policy ACCEPT)target prot opt source destination Chain OUTPUT (policy ACCEPT)target prot opt source destination **O sea, todo se permite tanto para la entrada como salida, siendo una configuración deficiente y tienen el cortafuego por gusto**. **Shorewall** por su parte tiene su fichero de configuración en **/etc/shorewall/shorewall.conf y los principales parámetros son:** • **STARTUP_ENABLED**. Por defecto viene desactivado Shorewall y se habilita poniendo STARTUP_ENABLED =Yes • Fichero de configuración **/etc/shorewall/zones** se define que se administrará con Shorewall y el tipo de zona. • Fichero de configuración **/etc/shorewall/interfaces** donde se definen las interfaces para las diferentes zonas. • Fichero de configuración **/etc/shorewall/policy** donde se establece como se accederá desde una zona hacia otra. • Fichero de configuración **/etc/shorewall/masq** donde se define a través de que interfaz o interfaces se habilitará enmascaramiento, o NAT, y para que interfaz o interfaces o redes se				

	aplicará dicho enmascaramiento. • Fichero de configuración **/etc/shorewall/rules** donde todos los puertos están cerrados de modo predefinido y en este fichero se habilitan según las reglas de accesos definidas.				
5.25	¿Se tiene definido un procedimiento para realizar periódicamente la verificación de la seguridad de la red con el fin de detectar posibles vulnerabilidades? 3.19 Coordinar con la dirección de redes de la OSRI la realización de diagnósticos remotos. 3.20 Realizar chequeo a la red de forma interna. 3.21 Empleando informaciones obtenidas en el chequeo de la red, intentaremos establecer conexiones con los (Router, modem-router y swhit) por los puertos abiertos, empleando para ello las contraseñas que vienen por defecto del fabricante y de ETECSA. Ejemplo: **Telnet 192.168.1.1 22** (Estamos tratando de conectarnos al dispositivo con IP 192.168.1.1 por el puerto 22).	Art. 67			
5.26	¿Se aplican mecanismos de seguridad que garanticen la confidencialidad, integridad, el control de acceso, autenticación y el no repudio según corresponda; en los servicios habilitados para intercambiar informaciones con otras redes o usuarios externos? ❖ ¿Existen mecanismos de identificación y autenticación para los diferentes servicios? ❖ ¿La información intercambiada no pone en riesgo su confidencialidad? ❖ ¿Se tienen definidos correctamente los derechos y permisos de las informaciones a intercambiar?	Art. 69			
5.27	¿Existe un procedimento para regular, autorizar y chequear el contenido de las informaciones que se colocan en servidores para su acceso público y	Art. 70			

	su correspondencia con los intereses de la propia entidad y del país? ❖ ¿Se tienen establecidos los responsables de definir las informaciones que se colocan en servidores de acceso público? ❖ ¿Tienen definidas las temáticas e informaciones a colocar en servidores para su acceso público? ❖ ¿Existen evidencias documentales sobre las comprobaciones realizadas a los Servidores que almacenan informaciones de acceso público? ❖ ¿Las informaciones colocadas en servidores de acceso público se corresponden con los intereses de la propia entidad y del país? ❖ ¿Se colocan programas o informaciones dirigidas a vulnerar los sistemas informáticos? ❖ ¿Se encuentran publicadas informaciones clasificadas y sensibles?				
5.28	¿Se tienen implementadas las medidas y procedimiento que garanticen la integridad y disponibilidad de la información que se coloca en servidores para su acceso público? ❖ ¿Se tienen definidos correctamente los derechos y permisos de las personas encargadas de depositar la información en los Servidores? ❖ ¿Se aplican métodos para chequear la integridad de la información? ❖ ¿Se tiene concebida la redundancia de la información?	Art. 70			
5.29	¿Existe constancia documental sobre la autorización de hospedar un sitio web en servidores ubicados en un país extranjero, donde se fundamenten los motivos que lo originaron?	Art. 71			
5.30	¿El sitio web hospedado en Servidores de un país extranjero, es un espejo o réplica del sitio principal radicado en los servidores de nuestro país?	Art. 71			
5.31	¿Se tienen establecidas las medidas de seguridad requeridas para garantizar la seguridad del sitio	Art. 71			

	web hospedado en Servidores de un país extranjero? ❖ Verificar la configuración de las réplicas o vías de actualización. ❖ Se aplican métodos de autenticación y protocolos seguros (Https, SSH, étc). ❖ Están definidas las responsabilidades, cargos y métodos para chequear posibles modificaciones de las informaciones o desfiguración del Sitio.				
5.32	¿Se colocan páginas o sitios Web desde entidades estatales en servidores extranjeros que ofrecen estos servicios de forma gratuita? ❖ Realizar búsquedas en Internet para determinar posibles violaciones al respecto.	Art. 72			
5.33	¿Los servidores que facilitan el acceso hacia o desde el exterior también tienen instalados los servicios de la red local? ❖ ¿Todos los servicios se encuentran implementados en una misma máquina? ❖ ¿Tienen definida una zona desmilitarizada (DMZ), donde independicen los servicios de la red local con la red externa? ❖ ¿Se tiene identificado el riesgo de tener todos los servicios en una misma máquina? ❖ ¿El o los servidores de aplicaciones informáticas, también aseguran la conectividad hacia o desde el exterior?	Art. 73			
5.34	¿En las políticas de seguridad se tienen definidos los servicios internos de la red coporativa que serán extrapolados a otras redes o usuarios externos, identificándose los puertos que serán empleados y las medidas de seguridad para garantizar el acceso por las personas autorizadas?	Art. 74			
5.35	¿Están autorizadas, por la máxima dirección de la entidad, las cuentas asignadas para recibir los servicios que ofrece la red mediante conexiones externas y están fundamentadas sus necesidades?	Art. 75			
5.36	¿Se tiene establecido un procedimiento para la aprobación, de forma excepcional, el	Art. 76			

	establecimiento de cuentas de correo electrónico desde la entidad en Servidores que se encuentran en el exterior del país? Debe contener: ❖ Nivel de aprobación. ❖ Fundamentación de su creación. ❖ Tipo de informaciones que se transmitirán. ❖ Plazo de vigencia. ❖ Responsabilidades y obligaciones del usuario autorizado. ❖ Medidas que serán adoptadas ante cualquier violación.				
5.37	¿Las cuentas de correo electrónico establecidas en servidores que se encuentran en el exterior del país, se encuentran aprobadas de forma escrita por el máximo dirigente y se fundamenta la necesidad de su utilización?	Art. 76			
5.38	¿En las políticas de seguridad se tiene definida la prohibición de vincular cuentas de correo electrónico de un Servidor de la entidad a un Servidor en el exterior del país y las medidas a adoptar ante cualquier violación?	Art. 77			
5.39	¿Se tienen vinculadas cuentas de correo electrónico de un Servidor de la entidad a un Servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través del mismo? 4.5 Verificar en las trazas del servicio de correo electrónico, sí algún usuario tiene habilitada la posibilidad de redireccionar sus mensajes a otras direcciones de correos que no se corresponden con la autorizad por la entidad.	Art. 77			
5.40	¿En las políticas de seguridad se tiene definida la utilización de las listas de discusión por correo electrónico y CHAT, así como las normas a seguir para su utilización?	Art. 78			
5.41	¿Los usuarios que está suscriptos a listas de discusión por correo electrónico y emplean el CHAT están autorizados por la máxima dirección de la entidad? ❖ Verificar en las trazas de internet los usuarios que emplean el servicio de CHAT y comprobar si están autorizados.	Art. 78 y 26			

	❖ Verificar en las trazas de correo electrónico la existencia de mensajes pertenecientes a listas de discusión y comprobar si están autorizados. ❖ ¿El empleo de los servicios de la lista de discusión y CHAT no representa beneficios para el desempeño del trabajador? ❖ ¿El empleo de los servicios de la lista de discusión y CHAT se utiliza para circular informaciones contrarias al interés social, la moral y las buenas costumbres?				
5.42	¿En las políticas de seguridad se tiene definida la prohibición de difundir a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas o que lesione la Seguridad Nacional? ❖ ¿Se define como una violación de seguridad informática?	Art. 79			
5.43	¿Se tienen implementados mecanismos de control que permitan detectar y obstaculizar la difusión de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas o que lesione la Seguridad Nacional? ❖ ¿Se tienen definidas reglas de filtraje por contenido, listas negras u otras variantes?	Art. 79			
5.44	¿En las políticas de seguridad se tiene definida la prohibición de enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (SPAM), ya sean de carácter informativo, cultural, comercial, social, con intenciones de engaño (HOAX) u otros?	Art. 80			
5.45	¿Se envían mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (SPAM y HOAX)? ❖ Verificar las trazas de correo electrónico para evidenciar la violación.	Art. 80			
5.46	¿Se tienen implementadas reglas de filtrado que impidan la sobrecarga de los canales de comunicaciones y la generación de cartas en cadena, restringiendo el envío o recepción de grandes volúmenes de información y la generación de mensajes a múltiples	Art. 81 y 82			

	destinatarios? Verificar qué: ❖ Existe redundancia del servicio de correo electrónico, principalmente en las entidades con mucho tráfico. ❖ Se establecen números máximos de destinatarios para un mensaje de correo electrónico. ❖ Se encuentra deshabilitada la respuesta del Servidor de correo a comandos como **EXPN** y **VRFY**, los cuales pudieran ser utilizados para revelar los nombres de usuarios locales a un **Spammer**. ❖ Se tienen deshabilitadas las notificaciones de entrega del mensaje, este es un mecanismo comunmente utilizado por quienes envían correo masivo no solicitado para verificar y confirmar la existencia de una cuenta activa. ❖ Está limitado el tamaño máximo permitido para la cabecera de un mensaje en bytes. Algunos programas utilizados para enviar spam generan cabeceras muy grandes. En las bibliografías consultadas sugieren **16 Kb** (16384 bytes). ❖ Está limitado el tamaño máximo permitido para un mensaje de correo electrónico en bytes. **En LINUX**: Para protegerse de una denegación de servicio (DoS) con ataques de “SYN” se recomienda habilitar su protección (Enable TCP SYN Cookie Protection). En el fichero **/etc/sysctl.conf** debe existir una línea de commando parecida a esta: # Enable TCP SYN Cookie Protection **net.ipv4.tcp_syncookies = 1** Es recomendable también tener deshabilitado el ICMP Redirect Acceptance, entonces en el fichero anterior aparecerá una línea de comando: **net.ipv4.conf.all.accept_redirects = 0** Para evitar el atque por engaño de IP (IP spoofing) se debe habilitar en el fichero				

	sysctl.conf: **net.ipv4.conf.all.rp_filter = 1**				
5.47	¿Se cumplen las regulaciones establecidas para brindar los servicios de conexiones remotas a otras personas naturales o jurídicas? Verificar qué: • Tienen establecidas las políticas de seguridad, medidas y procedimientos que garanticen la protección de los servicios a brindar. • Están implementados los mecanismos y procedimientos que aseguren la identificación del origen de las conexiones. • Se guardan las trazas del servicio RAS (conexiones remotas) y su conservación se garantiza por un tiempo no menor de un año. • Existe constancia documental donde los clientes de estos servicios conocen los requerimientos de seguridad y firman su compromiso de cumplimiento. • Las cuentas habilitadas se encuentran autorizadas. • Se aplican métodos de autenticación. **LINUX:** Las conexiones remotas pueden lograrse ya sea por **pppd** o **FreeRadius** u otra variante. El proceso de identificación y autenticación de PPPd se realiza de dos formas: **PAP** - Password Authentication Protocol y su configuración se encuentra en el fichero **/etc/ppp/pap-secrets**. Sí en vez de definir nombre de usuario y contraseña, ellos ponen asteriscos quiere decir que todos los usuarios del sistema (contenido del fichero passwd) pueden emplear el servicio RAS. Otros emplean **CHAP** y es parecido a lo anterior, lo que se busca el nombre de usuario y clave en	Art. 83			

	el fichero **/etc/ppp/chap-secrets**. CHAP es un protocolo más seguro que PAP, ya que nunca se envía la clave por la linea de transmisión sin cifrar. Sí utilizan un FreeRadius para la conexión remota entonces: 1. Buscar en **/etc/Radius o /etc/FreeRadius** y en su interior se encuentra el fichero de configuración. 2. Las trazas de este servicio se encuetran en **/etc/var/log**. **Para sistema operativo Windows:** Las conexiones RAS se pueden realizar de varias formas: **Una**: Empleando **Routing and remote access**. Esto se puede encontrar en **Inicio-Herramientas administrativas-Routing and remote access**. ➢ Puedes obtener las direcciones IP que asignan. ➢ Verificar si tienen habilitadas las trazas del servicio en **windos/system32/logfiles/** **Dos**: Sí tienen un **Active Directory**, en las cuentas de los usuarios en la propiedad **Dial-in**; le habilitan la propiedad de permitir conexiones remotas, call back y dirección IP fija. **Tercero**: Haciendo una configuración de conexión entrante, se observa en las conexiones de red y con click derecho se obtienen las propiedades y usuarios definidos.				
5.48	¿Se tiene definida una política de seguridad donde se prohiba la exploración o monitoreo de las redes públicas de transmisión de datos en busca de vulnerabilidades y/o información sobre	Art. 84			

	los usuarios legales de las mismas?				
5.49	¿Se tiene definida una política de seguridad donde se prohiba el acceso no autorizado o se agredan sistemas de cómputo conectados a redes públicas de transmisión de datos y la usurpación de los derechos de acceso de usuarios?	Art. 85			
5.50	¿Se realiza la exploración sin autorización o monitoreo de las redes públicas de transmisión de datos en busca de vulnerabilidades y/o información sobre los usuarios legales de las mismas? ❖ En la revisión de las estaciones de trabajo obtener evidencias sobre los programas instalados e identificar aquellos que son empleados para estos fines. En ocasiones en un fichero existente en plataforma LINUX (**bash_history**), principalmente del usuario root se han obtenido comandos ejecutados directamente desde la consola de comando para comprobar vulnerabilidades en diferentes redes informáticas y exploración de puertos abiertos especialmente de FTP, navegación y Chat. **Ejemplo**: nmap -v -sS -sU -sV -sR -O -p0 200.55.166.82	Art. 84 y 85			
Seguridad de los servicios (Otros apuntes particulares).					
DNS Es una base de datos distribuida y jerárquica que almacena la información necesaria					

para los nombres de dominio, empleándose el puerto **53** para responder las consultas. Los DNS operan a través de tres componentes: **Clientes DNS**, **Servidores DNS** y **Zonas de Autoridad**. Los Clientes DNS son programas que ejecuta un usuario y que generan peticiones de consulta para resolver nombres. Los Servidores DNS son servicios que contestan las consultas realizadas por los Clientes DNS. Hay dos tipos de servidores de DNS, uno Primario y otro Secundario. Las Zonas de Autoridad permiten al Servidor Primario cargar la información de una zona. Cada zona abarca al menos un dominio y en ocasiones sub-dominios, si estos últimos no son delegados a otras zonas de autoridad. La información de cada zona de autoridad incluye varios tipos de registros: **A** Registro de dirección que resuelve un nombre hacia una dirección Ipv4. **AAAA** Registro de dirección que resuelve un nombre hacia una dirección IPv6. **CNAME** Registro de nombre canónico, posibilita que un nombre sea alias de otro. **MX** Registro de servidor de correo que sirve para definir una lista de servidores de correo para un dominio y la prioridad existente entre éstos. **PTR** Registro de apuntador que resuelve direcciones IPv4 hacia el nombre, es decir, hace lo contrario al registro A. Se utiliza en zonas de Resolución Inversa. **NS** Registro de servidor de nombres, que sirve para definir una lista de servidores de nombres con autoridad para un dominio. **SOA** Registro de inicio de autoridad que especifica el Servidor DNS Primario.					
5.52	¿La configuración se corresponde con las direcciones IP y las zonas autorizadas? ❖ Verificar los Servidores DNS y las zonas definidas tanto directas como inversas. ❖ ¿Se encuentra apuntando a alguna dirección IP no autorizada u otras de otros países? En LINUX: ❖ Verificar la configuración de parámetros en el fichero **/etc/named.conf** ❖ Verificar configuración en **/var/named** ❖ Comprobar el fichero **/etc/resolv.conf**. Podemos utilizar el comando: $ **nslookup** osri.gov.cu Para conocer rápidamente el nombre del Servidor DNS que responde y de acuerdo a la configuración se puede conocer hasta la dirección IP. **Servidor**: servicios.hlg.desoft.cu Dirección: 192.168.2.254 (porque se corrió el comando en la red de Desoft y ese es el que	Art. 57 y 60			

	responde por el DNS) Para obtener información de un determinado dominio también se puede utilizar: # dig osri.gov.cu				
5.53	¿Se tiene implementado un sistema de redundancia para respaldar el servicio? ❖ Verificar si existen varios servidores para una zona. **En LINUX**: Sí existen servidores primarios y secundarios, el contenido del fichero de zona en el servidor primario es casi idéctico al secundario y su diferencia está en la definición del tipo de zona y que establece los servidores donde está hospedada la zona maestra. **Ejemplo**: Servidor secundario, configuración del fichero **/etc/named.conf** zone "osri.gov.cu" { **type slave**; file "osri.gov.cu.zone"; **masters** { **192.168.1.254**; };	Art. 57			
5.54	¿Los servidores definidos son los autorizados para transferir zona? **En LINUX**: En el fichero **/etc/named.conf** se emplea el parámetro **allow-transfer**, donde se especifican en el Servidor DNS Primario que servidores tendrán permitido ser servidores de nombres de dominio secundario, o sea, hacer transferencias.	Art. 57			
5.55	¿El servidor DNS permite consultas recursivas, lo que podría provocar una denegación de servicio (DoS) o denegaciones de servicios distribuidas (DDoS)? **En LINUX**: ❖ Verificar sí en el fichero **/etc/named.conf**, en su sección de opciones (options), aparece una línea de comando que defina la red, las redes o bien las ACL (listas de control de acceso) que tendrán permitido realizar **allow-recursion**. Para no	Art. 57			

	permitirse debe existir alguna configuración como esta: **Ejemplo**: options { directory "/var/named"; dump-file "/var/named/data/cache_dump.db"; statistics-file "/var/named/data/named_stats.txt"; forwarders { 192.168.0.1; }; forward first; **allow-recursion { 127.0.0.1; 192.168.0.0/24**; }; **Lo anterior hace que solo se puedan realizar consultas recursivas en el DNS desde 192.168.0.0/24 (mi red local)**				

5.56	¿Se gestionan dominios a través de redes públicas?
	En LINUX:
	❖ Sí gestionan dominios a través de redes públicas entonces debemos verificar si emplean claves cifradas en lugar de una dirección IP, debido a que esta última puede ser falsificada.
	
	Sí emplean este método se encontrará en **/var/named/** adicionalmente otros ficheros que contienen las claves cifradas, tanto para el servidor primario como secundario en el fichero **named.conf** tendría:
	key osri.gov.cu {
	algorithm HMAC-MD5;
	secret "NPuNuxvZAjtd3mriuygT8Q==";
	};
	zone "osri.gov.cu" {
	type master;
	file "osri.gov.cu.zone";
	allow-update { none; };
	allow-transfer { key osri.gov.cu; };
		Art. 57			

5.57	¿Se tienen definidos correctamente los permisos de los ficheros de zona? **En LINUX**:	Art. 57			

	Todos los ficheros de zona deben pertenecer al usuario **named**, a fin de que el servicio named pueda acceder a estos o bien modificarlos en el caso de tratarse de zonas secundarias.				
DHCP DHCP es un protocolo que permite a dispositivos individuales en una red de direcciones IP obtener su propia información de configuración de red (dirección IP, máscara, puerta de enlace, etc.) a partir de un servidor DHCP.					
5.58	¿Se emplea el servicio DHCP solamente para la red local? **En LINUX**: Revisar el fichero de configuración **/etc/sysconfig/dhcpd** y sí tuvieran limitada su utilización debería aparecer su definición en el parámetro **DHCPDARGS**. Ejemplo: Considerando que **eth0** es la interfaz de la red local, debe aparecer la línea de comando: # Command line options here **DHCPDARGS=eth0**	Art. 57 y 58			
INTERNET. **HTTP** es el protocolo y regularmente se utiliza el puerto **80**, estas comunicaciones se pueden intervenir con la utilización de un PROXY, puertas de enlace y túneles. **HTTPS** es la versión segura del protocolo HTTP y emplea el puerto **443.**					
5.59	¿Se establecen reglas de accesos para los usuarios autorizados? En plataforma LINUX se emplea como Proxy el **Squid** y es el más utilizado en los sistemas operativos GNU/Linux. **Ninguna versión anterior a la 2.5.STABLE6 se considera como apropiada debido a fallas de seguridad de gran impacto.** Revisar el fichero de configuración localizado en **/etc/squid/squid.conf** y los parámetros principales a tener en cuenta son: ❖ http_port (de modo predefinido Squid utilizará el puerto 3128).	Art. 57 y 58			

	❖ Lista de control de acceso: **acl** [nombre de la lista] src [lo que compone a la lista] ❖ Regla de control de acceso: Definen si se permite o no el acceso hacia Squid. Comprobar si existen reglas para controlar los tipos de navegación (nacional o internacional), límites de días de semana y horarios de navegación, descargas de ficheros, étc. Se aplican a las listas de control de acceso y la sintaxis básica es la siguiente: **http_access** [deny o allow] [nombre de la lista] ❖ Método de autenticación. **Con LDAP**: Buscar en el fichero de configuración de Squid la línea: auth_param basic program /usr/lib/squid/squid_ldap_auth -b dc=su-red-local,dc=cu 127.0.0.1 **Con el módulo NCSA**: Provee una autenticación muy sencilla a través de un fichero de texto, en el ejemplo sería el fichero claves y la línea del SQUID sería: auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/claves				
5.60	Comprobar en la revisión de las trazas la posible utilización de proxys anónimos para burlar las restricciones definidas para el servicio.	Art. 12 inc f) y 65			
Correo Electrónico. Se emplean los protocolos: **SMTP**: Es un protocolo a nivel de aplicación utilizado para la transmisión de correo electrónico a través de una conexión TCP/IP y trabaja con el puerto **25**. **POP3**: Es un protocolo a nivel de aplicación que permite recibir el correo electrónico a través de una conexión TCP/IP y trabaja con el puerto **110**. **IMAP**: Es un protocolo a nivel de aplicación utilizado para acceder al correo electrónico, a diferencia POP3, este permite accesos simultáneos desde múltiples estaciones de trabajo por el puerto **143**					
5.61	¿Se establecen reglas de accesos para los usuarios autorizados (nacional o internacional)?	Art. 20, 23 y 60			
5.62	¿Se encuentra desactivada la ejecución automática de los adjuntos al abrir el mensaje de	Art. 50			

	correo electrónico para evitar la propagación de programas malignos?				
5.63	¿Se está autenticando la cuenta de administración (root) a través de la red para revisar los mensajes originados por el sistema? ❖ Comprobar si tienen definidas alias para la cuenta de administración. En LINUX verificar el fichero **/etc/aliases**.	Art. 63			
5.64	¿Se tiene habilitada la autenticación para SMTP (Simple Mail Transfer Protocol) durante el envío de los mensajes, con el objetivo de evitar la suplantación de identidad?	Art. 69			
5.65	¿Se envian/reciben mensajes contentivos de claves de acceso u otro tipo de información sensible?	Art. 69			
5.66	¿En los ficheros del agente de transporte del correo (Mdaemon para Windows, SENDMAIL o POSTFIX para LINUX), se encuentra habilitado el mensaje de bienvenida que establece la conexión al servidor con el objetivo de ocultar el nombre y la versión empleada? **En LINUX**: El **postfix** es el más utlizado y el fichero de configuración es **main.cf** que se encuentra en **/etc/postfix**	Art. 69			
5.67	Realizar comprobaciones del servicio para identificar vulneravilidades, para ello se emplean informaciones obtenidas en los diagnósticos de la red sobre los puertos abiertos y nombres de cuentas de correo electrónico: ❖ Establecer una conexión escribiendo en la consola de comando: **Maquinamía**: telnet 127.0.0.1 25 **Servidor**: Trying 127.0.0.1... Connected to localhost.localdomain (127.0.0.1). Escape character is '^]'. 220 nombre.dominio ESMTP Postfix 8.13.1/8.13.1; Sat, 18 Mar 2010 16:02:27 -0600 **Maquinamía**: HELO localhost.localdomain **Servidor**: 250 nombre.dominio Hello localhost.localdomain [127.0.0.1], pleased to meet you	Art. 69			

	Maquinamía: MAIL FROM:<cuenta@localhost.localdomain> **Servidor**: 250 <cuenta@localhost.localdomain>... Sender ok **Maquinamía**: RCPT TO:<root@localhost.localdomain> **Servidor**: 250 <root@localhost.localdomain>... Recipient ok **Maquinamía**:DATA **Servidor**: 354 Enter mail, end with "." on a line by itself **Maquinamía**: Subject: Mensaje de prueba From: cuenta@localhost.localdomain To: root@localhost.localdomain Hola. Este es un mensaje de prueba. . (Este punto debe escribirse para terminar el contenido del mensaje) **Servidor**: 250 Message accepted for delivery **Maquinamía**: QUIT Servidor: 221 nombre.dominio closing connection Servidor: Connection closed by foreign host.				
LDAP Se emplea el puerto **389 y 636** para LDAPS. Es un servicio de directorio, muy similar al Active Directory de Windows.					
5.68	El fichero de configuración se encuentra en **/etc/openldap/slapd.conf** ó **/etc/ldap.conf** ❖ Verificar el método de autenticación de los usuarios de la red y comprobar sí el usuario **root** tiene asignado una contraseña. En las líneas de ese fichero debe existir unas líneas que tenga algo como esto: database bdb suffix **"dc=dominio de la red,dc=cu"** rootdn **"cn=Administrador,dc= dominio de la red,dc=cu"** **rootpw**	Art. 57 y 58			
APACHE Es un servidor HTTP de código abierto y que funciona en Linux, Windows, Novell Netware y otras plataformas, puerto 80 y 443.					
5.69	El fichero de configuración en LINUX se encuentra en **/etc/httpd/** y en **/etc/httpd/conf.d/** pueden encontrarse otros ficheros de configuraciones específicas como por ejemplo	Art. 58			

	incluir directorios virtuales, redirección de directorios, étc. ❖ Verificar sí tienen establecidos los atributos de **lectura** y **escritura** solo para el usuario **apache** a los ficheros que contienen claves de acceso (**.htaccess**). Debe tener **600** para **apache**:**apache** Este proceso de autenticación se puede hacer en un fichero **.htaccess** con la sintaxis siguiente: AuthName "Acceso por claves" AuthType Basic require valid-user AuthUserFile /cualquier/ruta/claves **Por lo tanto, debemos buscar si existen ficheros de este tipo y comprobar sus permisos.**				
MYSQL Es un sistema de gestión de base de datos SQL y emplea el puerto **3306**					
5.70	Cuando se inicia por primera vez el MySQl, el usuario **root** no tiene asignada una clave de acceso. ❖ Para comprobar si existe esta vulnerabilidad realice lo siguiente en una consola de comando: # mysql Entonces saldrá el intérprete de comandos de MySQL y escribes: > use mysql > show tables; (muestra las tablas de la base de datos mysql) > select * from user; (muestra el contenido de la tabla user) Entonces nos fijamos sí el suario **root** no tiene asignada una clave de acceso, de ser así entonces permite que cualquiera que se identifique como root en el sistema tendrá acceso a todo en MySQL. Por razones de seguridad, es muy importante asignar una clave con el comando: mysqladmin -u root password nueva	Art. 58			

SSH SSH (Secure Shell) es un conjunto de estándares y protocolo de red que permite establecer una comunicación a través de un canal seguro entre un cliente local y un servidor remoto. Garantiza confidencialidad e integridad en la transferencia de los datos utilizando criptografía. Emplea el puerto **22** por defecto.					
5.71	**En LINUX**: Fichero de configuración se encuentra en **/etc/ssh/sshd_config** **Parámetro Port**. Una forma de elevar considerablemente la seguridad al servicio de SSH, es cambiar el número de puerto utilizado y que solamente sea conocido por los administradores. Puede elegirse cualquier otro puerto entre el 1025 y 65535. **Parámetro ListenAddress**. Por defecto, el servicio de SSH responderá peticiones a través de todas las interfaces del sistema. Para garantizar mayores niveles de seguridad se recomienda limitar el acceso desde determinadas estaciones de trabajo de la red local. Ejemplo: ListenAddress 192.168.1.254 **Parámetro PermitRootLogin**. Establece si se va a permitir el acceso directo del usuario **root** al servidor SSH. **Sí permiten el acceso hacia el servidor desde redes públicas, constituye una vulnerabilidad potencial**. Por lo que es necesario definir este parámetro con el valor **no**. Ejemplo: PermitRootLogin no **Parámetro X11Forwarding**. Establece si se permite o no la ejecución remota de aplicaciones gráficas. Si accedemos hacia el servidor desde la red local se podría quedar con	Art. 58			

	el valor **yes**. Si permitien accesos hacia el servidor desde redes públicas es recomendable utilizar este parámetro con el valor **no**. Ejemplo para la red local: X11Forwarding yes **Parámetro AllowUsers**. Permite restringir el acceso por usuario y, opcionalmente, desde qué estación de trabajo. Ejemplo: AllowUsers julio karel Esto restringe el acceso para los usuarios julio y karel, desde cualquier computadora. Otro ejemplo: AllowUsers julio@192.168.11.2 karel@192.168.11.3 Se restringe el acceso para los los usuarios julio y Karel desde las computadoras con direcciones IP 192.168.11.2 y 192.168.11.3 Para acceder a través de la consola de comandos hacia un Servidor se escribiría: ssh usuario@servidor ❖ Utilizar claves públicas, en lugar de claves de acceso resulta una técnica más segura para autenticar este servicio.				
FTP Es el protocolo de transferencia de archivos es uno de los más utilizados empleando los puertos **20** y **21**.					
5.72	**En LINUX**: Se emplea mucho **Vsftpd** (Very Secure FTP Daemon) y sus valores predeterminados son muy seguros en comparación con ProFTPD y Wu-ftpd. El fichero de configuración se ubica en **/etc/vsftpd/vsftpd.conf** **Parámetro anonymous_enable**. Se utiliza para definir si se permitirán los accesos **anónimos** al servidor. **Parámetro local_enable**.	Art. 58 y 69			

	Establece si se van a permitir los accesos autenticados de los usuarios locales del sistema. **Parámetro write_enable**. Establece si se permite el mandato write (escritura) en el servidor. **Parámetro anon_upload_enable** Específica si los usuarios anónimos tendrán permitido subir contenido al servidor. Por cuestiones de seguridad no debe habilitarse esta opción, por lo que debe tener: anon_upload_enable=NO **Parámetro anon_mkdir_write_enable** Específica si los usuarios anónimos tendrán permitido crear directorios en el servidor. Igualmente al anterior no es una función deseada y se desactiva anon_mkdir_write_enable=NO **Parámetro ftpd_banner**. Este parámetro sirve para establecer la bienvenida que será mostrado cada vez que un usuario acceda al servidor. **Parámetro anon_max_rate**. Se utiliza para limitar la tasa de transferencia en bytes por segundo para los usuarios anónimos, algo sumamente útil en servidores FTP de acceso público. anon_max_rate=5120 (En este caso se limita la tasa de transferencia a 5 Kb por segundo para los usuarios anónimos) **Parámetro local_max_rate**. Se limita la tasa de transferencia en bytes por segundo para los usuarios locales del servidor. **Parámetro max_clients**. Establece el número máximo de clientes que podrán acceder simultáneamente hacia el servidor FTP. max_clients=5 (Se limita el acceso a 5 clientes simultáneos)				

	Parámetro max_per_ip. Establece el número máximo de conexiones que se pueden realizar desde una misma dirección IP. max_per_ip=5				
5.73	¿Después de realizarse descargas de ficheros se verifican éstos con el objetivo de identificar una posible contaminación de virus informáticos?	Art. 50			
Seguridad de redes inalámbricas.					
	¿Verificar sí se encuentra visible el SSID (Service-Set Identifiers) que es el nombre de la red inalámbrica disponible? ¿Tienen implementado algún mecanismo de cifrado? Herramientas para comprobar la seguridad: ❖ KisMAC ❖ WepCrack ❖ Kismet ❖ ssidsniff ❖ WarDrive ❖ APTools ❖ AirIDS ❖ Wellenreiter Los datos deben viajar cifrados por el aire, para evitar que equipos ajenos a la red puedan capturar datos mediante escucha pasiva. métodos para lograr la configuración segura de una red inalámbrica Filtrado MAC: Este método consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Es muy inseguro porque las direcciones MAC viajan sin cifrar.				

	WEP, logra proteger los datos que se transmiten mediante cifrado (40 o 128 bits); pero no tiene servicio de autenticación. VPN (Red privada virtual), la parte de la red que maneja el acceso inalámbrico debe estar aislada del resto de la red coorporativa; mediante el uso de una lista de acceso adecuada en un enrutador, o agrupando todos los puertos de acceso inalámbrico en una VLAN si se emplea switching. Dicha lista de acceso y/o VLAN solamente debe permitir el acceso del cliente inalámbrico a los servidores de autorización y autenticación de la VPN. WPA, mejora el cifrado de los datos y ofrecen un mecanismo de autenticación. La clave de cifrado se cambia entre el punto de acceso y el cliente cada cierto tiempo. WPA2, la seguridad es muchísimo más robusta y utiliza el algoritmo de encriptación AES; éste requiere un hardware de mayor prestación y provoca que los Puntos de Accesos anteriores al 2006 no se pueden utilizar, porque desde esa fecha constituye WPA2 un requisito obligatorio para todos los productos WIFI.				
Seguridad de las Aplicaciones y Bases de Datos					
5.7	¿Se encuentran los programas fuentes en la misma ubicación donde se ejecuta el programa compilado?	Art. 42			
5.7	¿Existen manuales y/o procedimientos de seguridad para las aplicaciones informáticas?	Art. 43			
	¿Está habilitado algún método de identificación y autenticación de los usuarios para acceder a la aplicación y la base de datos?	Art. 45			
	¿Los programas, bases de datos y ficheros que conforman el sistema están instalados en el disco duro de la computadora, en un directorio con acceso restringido solamente a los usuarios	Art. 48			

	autorizados?				
	¿Son los usuarios autorizados los que tienen acceso a las aplicaciones y bases de datos?	Art. 48			
	¿Está habilitada la opción de auditoría para las bases de datos?	Art. 48 y 58			
	¿Tienen los usuarios los permisos y derechos correctos sobre las bases de datos, atendiendo el cargo y funciones que desempeñan?	Art. 42 y 48			
	¿La información contenida en el fichero de palabras claves se encuentra cifrada, de forma tal que al editar el contenido del mismo no puedan conocerse las claves asignadas?	Art. 47 inc e)			
	¿Las claves de acceso de administración del sistema son de uso exclusivo del personal en funciones de administración?	Art. 48			
	¿Existe un documento escrito que defina los niveles de acceso de los usuarios, roles asignados y está aprobado por el jefe inmediato?	Art. 48			
	¿El acceso para la manipulación, modificación o edición de las bases de datos se logra solamente a partir de las opciones que brinda para ello el propio sistema?	Art. 48			
	Obtener las cuentas creadas en el sistema informático y realizar el análisis en busca de: – Obtener las cuentas creadas y sus roles de accesos, analizando su correspondencia con el cargo que ocupan. – Cuentas de usuarios pertenecientes a trabajadores que cesaron sus relaciones laborales. – Si tienen definido el tiempo de expiración de las cuentas. – Si todas las cuentas tienen password asignadas. – Si cada usuario tiene una password personal (no se comparten). – Si tienen definida la longitud mínima de la password y no menor de 6 caracteres	Art. 47 Art. 42 Art. 46 Art. 47 inc c)			
	¿La aplicación cuenta con procedimientos programados (Trazas) que permitan conocer la ocasión en que las personas autorizadas hacen uso de la misma y las funciones que emplean?	Art. 43			
	¿Desde el sistema se posibilita la realización de	Art. 53			

	salvas de la información?				
	¿Existe una copia de seguridad de los programas fuentes de la aplicación, la que se encuentra guardada fuera del área o local donde se encuentra instalado el sistema informático?	Art. 54			
	¿Se realizan restauraciones de las salvas con regularidad para asegurar el funcionamiento adecuado del proceso de Backup y restauración? ❖ ¿Se encuentran los Backup en las ubicaciones definidas para esos efectos (ubicación física y lógica de la información? ❖ ¿Se tienen documentados los Backup realizados, responsables, fechas de realización y su estado?	Art. 53 y 54			
	¿Las trazas de los eventos realizados sobre las bases de datos se encuentran habilitadas y garantizan su conservación por un período mínimo de un año? ❖ En base de datos (BD) SQL, abrir la consola de administración SQL SERVER, entonces se escoge la BD a analizar, damos clik derecho y escogemos propiedades; entonces en la pestaña que dice Transaction Log verificar el tamaño del fichero y su ubicación.	Art. 58			
	¿Se tiene delimitado las funciones de desarrollo, prueba y producción de Software? Consideramos que deben incorporarse estos puntos a controlar en aquellas entidades donde diseñan Softwares u otras aplicaciones específicas (DESOFT, SEGURMATICA, UCI, Universidades, étc): a) ¿Se definen y documentan los procesos establecidos para transferir el software del ambiente de desarrollo al de producción? b) ¿El software de desarrollo y el de producción se encuentran funcioando en computadoras diferentes? c) ¿Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema son accedidas solamente por los usuarios pertenecientes al área de desarrollo? d) ¿Se tienen definidos perfiles de usuario	Art. 42 y 43			

	diferentes para los sistemas en producción y de prueba? e) ¿En las pruebas del sistema no se aplican informaciones sensibles de una entidad? f) ¿Se tiene definido un proceso de cuarentena para someter los sistemas a pruebas? ¿En las pruebas se comprueba la disponibilidad del sistema, seguridad, efectos sobre otros sistemas y facilidades del usuario? g) ¿Existe un registro de auditoría para el control de las actualizaciones de los programas en producción? h) ¿Se conserva la versión anterior del Software de aplicación como una medida de contingencia?				
	¿Existe un procedimiento escrito donde se detallen los pasos a seguir para la recuperación de las aplicaciones y bases de datos ante la ocurrencia de fallas o desastres?	Art. 87			

Anexo No. 4

Ministerio de Auditoría y Control

INDICACIONES METODOLÓGICAS PARA LA AUDITORÍA A LOS SISTEMAS DE INFORMACIÓN

Objetivos:

- Brindar al auditor una estrategia metodológica para el desarrollo de la auditoría a sistemas de información con particular énfasis en los sistemas contables-financieros, a través de los anexos siguientes:

Anexo 1 – Indicaciones para auditoría a los sistemas contables financieros

Anexo 2 – Indicaciones para auditoría haciendo énfasis en la seguridad asociada a los sistemas contables-financieros.

- Servir de apoyo para los auditores que no cuenten con experiencia suficiente en este tipo de Auditoría.
- Facilitar la función de supervisión.
- Auxiliar en la labor de entrenamiento para mejorar la eficacia y la eficiencia del personal que se desempeña en esta especialidad.

Objetivos generales de la auditoría a los sistemas de la información

- Verificar el cumplimiento de las políticas, normas y procedimientos que rigen el uso de los sistemas de información.
- Comprobar la seguridad razonable sobre los recursos de tecnologías informáticas (datos, tecnologías, instalaciones, personal y aplicaciones), cumpliendo con los objetivos de control y los objetivos generales de estos sistemas.
- Que la información que se procese sea oportuna y confiable.
- Verificar el grado de privacidad del ambiente informático.

Áreas de interés que deben verificarse:

- Evaluar los controles de acceso, entrada de datos, procesamiento, salidas de datos modificaciones, calidad y seguridad de la información.

- Exactitud del procesamiento.
- Incidencias en el Control Interno, Contable y Administrativo.
- Cultura organizacional.
- Competencia profesional del personal informático.
- Que los controles de seguridad y continuidad estén establecidos tanto en los procesos manuales como automatizados.
- La existencia de procedimientos efectivos para controlar los datos recibidos y los enviados.
- La dirección y administración de las Tecnologías de Información relacionadas a estos sistemas.
- Cumplimiento de las políticas y plan de seguridad informática
- Segregación de funciones.
- Que estén bien definidos y se cumplan las políticas y planes informáticos.
- Que se cumplan los contratos por servicios y a terceros.
- Que los trabajos de planeamiento, adquisición, desarrollo, operación y mantenimiento de los sistemas estén documentados y controlados.
- El aprovechamiento y rendimiento de los demás sistemas.
- Administración y seguridad de las redes.

ANEXO 1 – INDICACIONES PARA LA AUDITORIA A LOS SISTEMAS CONTABLES FINANCIEROS

- Chequear que la entidad o centros que explotan sistemas y programas contables financieros sustentados en las tecnologías de la información impriman al cierre del ejercicio económico anual, los registros contables con independencia del sistema que esté en explotación y a conservar los listados y la información en soporte electrónico según la legislación vigente.

- Revisar que los sistemas contables financieros soportados sobre las tecnologías de la información, cuenten con una Certificación de la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones.

GENERALES DE LOS REQUERIMIENTOS DE LOS SISTEMAS CONTABLES

RESPONSABILIDADES

- Debe comprobarse si se cumplen las siguientes obligaciones principales de los usuarios de las tecnologías de la información para la Explotación de un Sistema Contable Financiero en una entidad:

  a) Que tengan la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.

  b) Cuenten con la autorización expresa del jefe facultado, para obtener acceso a cualquier activo o recurso.

  c) Que no divulguen la información a que tiene acceso sin la autorización del Jefe facultado.

  d) Que cumplan los procedimientos establecidos para el empleo de las contraseñas y para la salva de programas y datos.

  e) Que no introduzcan ni utilicen en las tecnologías ningún producto ni modifiquen la configuración de las mismas, sin la correspondiente autorización del jefe facultado.

  f) Que no intenten transgredir ninguna de las medidas de seguridad establecidas.

  g) Que no protejan las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada, dañada o usada la información que contiene o utilizado el sistema al que esté conectada.

  h) Si Informan al dirigente facultado de cualquier anomalía de seguridad detectada.

IDENTIFICACIÓN, AUTENTICACIÓN Y CONTROL DE ACCESO

- Verificar que el acceso de los usuarios a los sistemas contables financieros de una entidad esta aprobado previamente por la dirección de la misma y constar evidencia documental de ese acto.
- Chequear si el equipamiento utilizado en los sistemas contables financieros es utilizado por personal que no esté debidamente autorizado.
- Verificar si en la entidad están definidos los procedimientos que se requieren para otorgar o suspender el acceso de los usuarios a los sistemas contables financieros y los perfiles de trabajo de los mismos. Revisar si incluyen un listado de usuarios autorizados con sus derechos de acceso, garantizando la eliminación de aquellos que ya no los requieran por razones de trabajo o por no laborar en la entidad, así como de los identificadores, junto a todos los derechos de acceso que le fueron concedidos.
- Verificar si las tecnologías de información utilizadas en la explotación de los sistemas contables financieros tienen implementados mecanismos para identificar y autenticar a los usuarios, así como para garantizar el registro y conservación de todos los accesos e intentos fallidos de acceso.
- Comprobar si las contraseñas para la protección de los sistemas y la protección del propio usuario cumplen las siguientes condiciones:
    a) Si son privadas e intransferibles.
    b) Si su estructura y fortaleza esta en correspondencia con el acceso que protegen.
    c) Chequear que no sean visualizadas en pantalla mientras se teclean.
    d) Chequear que no sean almace/nadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información.
    e) Verificar que se guarda copia de las mismas, de forma que se garantice su privacidad, para su empleo como excepción en caso de ausencia del usuario.

INTEGRIDAD DE LOS SISTEMAS, FICHEROS Y DATOS

- Verificar si están implementados los mecanismos de seguridad que eviten la modificación, destrucción y pérdida de los ficheros y datos vinculados con los sistemas contables financieros.
- Comprobar si están establecidos, por las entidades, las medidas para proteger los programas del sistema y sus procedimientos de control para evitar que puedan ser violados, borrados o modificados con el fin de evadir los controles de seguridad.
- Comprobar si los programas, ficheros y datos de los sistemas contables financieros, incluyendo las copias de respaldo cumplen lo siguiente:
    a) Que no sean accedidos públicamente sin la debida autorización.
    b) Que los accesos temporales estén plenamente justificados y aprobados, así como ser eliminados inmediatamente después de terminar la necesidad de su uso.
    c) Que las actividades de uso y acceso realizadas por los usuarios, tienen que estén registradas y revisadas.
- Verificar si se garantiza la existencia de pistas o rastros de seguimiento que posibiliten las investigaciones más comunes que se realizan sobre las operaciones, tales como las cuentas que fueron afectadas por una transacción, la emisión de una factura, las retenciones que afectaron el salario devengado, y otras similares.
- Verificar si incluye facilidades de empleo del sistema (información clara, navegación intuitiva, etc.)
- Chequear que permitan la interoperabilidad entre los diferentes módulos del sistema
- Chequear si el sistema deberá contar con ayuda en línea para facilitar el trabajo de los usuarios.
- Si cuentan con un Manual de Usuario y un Manual de Explotación.
- Si cuentan con garantías de soporte, mantenimiento y capacitación para su explotación.
- Verificar que cuenten con la posibilidad de ser modificado y/o actualizado a versiones superiores, contando con la correspondiente documentación y los ficheros fuentes.

TRABAJO EN RED Y SISTEMAS MULTIUSUARIOS

- Comprobar si los Sistemas pueden trabajar en red y ser multiusuarios.

- Verificar en las tecnologías de información que brindan servicio a varios usuarios, como sistemas multiusuarios, servidores de bases de datos, se implementan mecanismos de control que permitan contar con una traza o registro de los principales eventos que se ejecuten, por lo que:
    a) Chequear si se controla el acceso al servidor o a las terminales.
    b) Chequear si esta debidamente compartimentado y controlado el acceso a los ficheros o bases de datos de los sistemas de forma tal que se garantiza la identificación de dicho acceso.
- Verificar si se utiliza los servicios Web como filosofía de trabajo.

PROCEDIMIENTOS DE SALVA DE LOS FICHEROS DE DATOS Y EL SISTEMA

- Verificar si en la entidad se establecen los procedimientos que garantizan:
    a) La obtención de copias de seguridad actualizadas de programas y datos.
    b) La frecuencia con que se realicen.
    c) Los responsables de la ejecución de los procedimientos.
    d) La cantidad de copias que tienen, según su importancia.
    e) Si cada salva esté adecuadamente identificada.
    f) Se mantengan copias de seguridad para datos y programas en algún soporte magnético externo.
    g) Si las copias de seguridad se conservan en locales alejados de donde se procesa habitualmente.

GENERALES PARA LA EVALUACION DE LOS SISTEMAS CONTABLES

Estas verificaciones sólo se realizan a aquellos sistemas que no cuenten con la certificación de la Agencia de Control y Supervisión del Ministerio de la Informática y las Comunicaciones. Si de tener la entidad la certificación, pero durante la auditoría se detectan errores e irregularidades, estas deben informarse a los ministerios de Finanzas y Precios y de la Informática y las Comunicaciones.

Para evaluar la integralidad del sistema contable financiero se deben tener en cuenta los aspectos siguientes:

a) Intercambio de información entre módulos de forma automática y por opciones. Ej.: comprobantes transferidos al módulo de contabilidad que hayan sido

generados en otros módulos.

b) Ejecución de procesos condicionada a resultados de procesamientos de la información en otros módulos. Ej.: no permitir el cierre de determinado periodo contable, en el módulo de contabilidad, si no se ha ejecutado el cierre de ese periodo en los demás módulos.

c) Funcionamiento en regímenes monousuario y multiusuario.

- Deben validarse todos los campos que contengan datos, según su rango y tipo.
- Capacidad de dejar trazas de los procesos utilizados por el período de tiempo establecido para la conservación de la información contable.
- Capacidad de importar y exportar bases de datos desde y hacia otras empresas vinculadas al mismo sistema informativo o desde y hacia otros sistemas.
- Capacidad de dejar trazas de las salvas y restauras por el período de tiempo establecido para la conservación de la información contable.
- Instalador.

  a) Posibilidad de instalación general o por módulos.

  b) Capacidad de condicionar la instalación por módulos a la instalación de un módulo asociado determinado.

  c) Posibilidad de ser instalado en múltiples empresas que trabajarían bajo un mismo fondo informativo.
- Debe existir un Manual de Usuario y un Manual de Explotación. (Ver Glosario de Términos).

  a) Evidencia de la actualización permanente de toda la documentación del sistema.
- Sistema operativo en que está soportado.
- Los reportes han de tener la posibilidad de salir por pantalla, impresora o diferido, indistintamente.
- En todas las pantallas de captación debe existir una ventana donde se registre el número del documento primario como un dato más.
- En los reportes debe existir la posibilidad de reimpresión y de selección de un rango de páginas a imprimir.
- Todos los módulos han de tener procesos de reindexación automática y opcional.
- Los textos de los mensajes de error y de advertencia han de ser claros y precisos en lenguaje de fácil comprensión.

- Cada proceso tiene que disponer de una ayuda en línea que dé una explicación adecuada de su funcionamiento.
- Los reportes básicos, requeridos por el fondo informativo contable, han de estar nominalizados y programados en opciones. Otros reportes que se requieran como apoyo al desempeño contable pudieran ser solicitados a través de pantallas con parámetros al efecto.
- Si tiene la posibilidad de registrar operaciones en múltiples monedas, debe ajustarse a lo establecido en las normas contables cubanas.
- Los reportes deben contener la fecha del período a imprimir y la fecha de impresión, así como la numeración de todas sus páginas, título del reporte y nombre de la entidad.
- Opción de consolidación de estados financieros.

MÓDULO DE CONTABILIDAD

Verificar en el módulo de contabilidad los aspectos siguientes:

Procesos fundamentales que deben conformar este módulo:

a) Apertura de saldos en el mayor y cierre de la apertura.

b) Operaciones.

c) Informes.

d) Cierres mensual y anual.

- La apertura de saldos en el mayor, cuya fuente ha de ser un balance de comprobación, debe estar condicionada a que no se haya efectuado el cierre de la misma. Otros saldos que se incorporen o actualicen tienen que ser absolutamente a través de comprobantes de operaciones.
- El cierre de la apertura de saldos del Mayor tiene que estar condicionado a que esté cuadrado el Balance que dichos saldos generan.
- El proceso de operaciones debe contener al menos las siguientes opciones:

  a) Pantalla de captación de las partidas que conforman un comprobante así como de las correcciones inherentes.

  b) Cuadre automático del comprobante en su captación.

  c) Posibilidad de salir de la pantalla de captación independientemente a que se haya concluido el pase de todas las partidas del comprobante.

d) Borre de un comprobante mientras no haya sido traspasado al mayor.

e) Imposibilidad de borrar las cuentas o subcuentas con movimientos y con saldos durante el ejercicio económico.

f) Traspaso del comprobante al mayor a través de opción.

g) Información sobre los comprobantes captados cuya situación es:

- Traspasados al mayor.
- No traspasados al mayor.
- No cuadrados.

h) Visualización de un comprobante de los periodos contables de los tres ejercicios fiscales anteriores, como mínimo.

i) Posteo (traspaso al mayor), bajo el cumplimiento de las siguientes premisas:

- Proponer el número consecutivo de manera automática.
- Que los comprobantes estén cuadrados.
- Que la fecha de los comprobantes esté en correspondencia
- con el periodo contable vigente.
- Que previo a iniciarse la operación de posteo y como parte integrante de la misma el sistema emita en un registro impreso o visual del comprobante o lote de comprobantes a postear.
    - Inclusión en un Fichero Histórico de las operaciones posteadas.

- En el proceso de Informes deben ser emitidos básicamente los siguientes reportes:

a) Edición de comprobantes con el detalle de la operación para cualquier período.

b) Consultas al mayor, donde se muestre de cada cuenta solicitada, el saldo inicial, el saldo de cada mes desde enero del año en curso hasta el mes vigente y el saldo hasta la fecha.

c) Listado del fichero histórico donde se muestre, según rango de cuentas y de meses solicitados, el detalle siguiente de las operaciones efectuadas:

- Código de la cuenta.
- Descripción de la cuenta.
- Saldo inicial del rango solicitado.
- De cada comprobante incluido en el rango solicitado: el número, la fecha, el módulo de procedencia, detalle de la operación, el importe deudor o acreedor de la operación y el saldo resultante en cada operación.
- Totales de los débitos y los créditos.

d) Balance de comprobación a nivel de cuentas y subcuentas.

e) Listado del fichero histórico de comprobantes para cualquier período.

- Los procesos de cierres mensual y anual deben estar condicionados a los siguientes eventos:

  a) Cierre mensual:

  - El nuevo periodo contable debe ser el inmediato siguiente al periodo contable vigente.
  - Solo puede efectuarse cuando hayan sido cerrados los demás módulos.
  - No deben quedar Comprobantes pendientes de posteo.
  - Aviso para salva de información.

  b) Cierre anual:

  - Haberse realizado el cierre del último mes del periodo contable.
  - Que se haya efectuado el cierre contable.
  - Que se hayan emitido el resto de los Estados Financieros establecidos.
  - Aviso para salva de información.

- Imposibilidad de reabrir un período que previamente haya sido cerrado.
- Aspectos a tener en cuenta al emitir los Estados Financieros y cualquier otra información.

  Se debe chequear la confección de parámetros:

  a) Modelos a generar.
  b) Conceptos de filas y columnas de cada modelo según las normas vigentes.
  c) Estructuras de los informes según las normas vigentes.
  d) Traslado de saldos desde las correspondientes bases de datos procedentes del módulo de contabilidad.
  e) Tecleo de datos que no se encuentren registrados en base alguna.
  f) Generación de totales y subtotales o su traslado desde las correspondientes bases de datos procedentes del módulo de contabilidad.
  g) Debe tener elaboración automática de todos los modelos predefinidos a partir de los parámetros confeccionados.
  h) La emisión de los informes correspondientes debe ser de los modelos elaborados, ficheros históricos de cualquier período, con representación impresa y por pantalla.

MÓDULO DE EFECTIVO CAJA Y BANCO

Verificar en el módulo de efectivo caja y banco los aspectos siguientes:

- Debe permitir asociar cuentas contables con cuentas bancarias.
- Emitir la conciliación bancaria, por cualquier método, por cada cuenta.
- Permitir el análisis y elaboración de flujos de caja.
- Emitir los comprobantes de operaciones de los hechos económicos asociados con el movimiento del efectivo y su traspaso al módulo de contabilidad.

MÓDULO DE INVENTARIOS

Verificar en el Módulo de Inventarios los aspectos siguientes:

Procesos fundamentales que deben conformar este módulo:

  - Método de valoración de los inventarios.
  - Ficheros Maestros.
  - Apertura.
  - Movimientos.
  - Posteo.
  - Registro de operaciones.
  - Operaciones contables.
  - Informes.
  - Cierres.

- Datos que deben estar en las bases de datos que corresponda, pero que no deben faltar.

  a) Sobre los almacenes. Cada registro debe incluir el código del almacén, su descripción y su estatus (abierto o cerrado).

  b) Sobre los Productos. Cada registro debe incluir:

  - Código del producto.
  - Claves de ajuste. Cada registro debe incluir un tipo de ajuste con su código.
  - Código del almacén en que se ubica.
  - Cuenta - subcuenta de inventario.
  - Descripción del producto.
  - Unidad de medida de despacho.
  - Precio Unitario.

- Cantidad de existencia en la apertura y/o posteriores movimientos.
- Fecha de apertura.
- Fecha del último movimiento efectuado.
- Importe de la existencia en la apertura y/o en la fecha actual.
- Sección, estante y casilla en que se ubica dentro del almacén
- Validación que impida duplicidades en captación.

- Apertura.

  Debe incluir las opciones de apertura y cierre de los almacenes definidos.
  - En la de apertura se deben registrar todos los saldos en existencia que se encuentran ubicados en determinado almacén.
  - En la de cierre, una vez ejecutada, impide la inclusión de artículos (productos) adicionales. La inclusión de nuevos saldos solamente puede hacerse mediante la correspondiente opción de movimiento.

- Movimientos

Se debe comprobar la captación de los movimientos de entradas, salidas y transferencias, donde se registran los siguientes datos:

- Código del almacén.
- Número y tipo del documento que da lugar a la operación.
- Número de prelación, con vistas a garantizar la actualización de un producto en cuestión con los movimientos de inventario en el mismo orden en que se efectuaron en el almacén.
- Fecha del documento.
- Código del producto.
- Unidad de medida.
- Cantidad.
- Existencia final según documento.
- Importe, calculado automáticamente en el proceso.
- Existencia en almacén una vez efectuado el movimiento.
- Diferencia, calculada automáticamente, entre la existencia que debe quedar en el submayor cuando se actualice el saldo con el movimiento efectuado y la existencia manifestada en el documento.
- Centro de costo afectado por el movimiento de salida o devolución
- Cuenta de contrapartida a contabilizar el movimiento.

- Posteo.

  Se debe verificar en el traspaso al submayor de los movimientos de productos cuyos saldos no hayan mostrado diferencia en la captación.

  Verificar en este proceso que debe hacerse la actualización del precio promedio, emitir un listado de la misma y otro listado mostrando las diferencias surgidas entre las existencias reportadas por el almacén y las del submayor para su investigación.
- Registro de operaciones.

  Chequear que se emita un registro numerado del lote de los movimientos posteados separados por su tipo (entradas, salidas, devoluciones, transferencias).
- Operaciones contables.
    - Debe confeccionarse un comprobante de operaciones por cada tipo de los movimientos del lote posteado al submayor y su traslado al módulo de contabilidad.
    - Trasladar al módulo de cobros y pagos las ventas y las compras incluidas en el lote posteado.
- En el proceso de Informes deben ser emitidos básicamente los siguientes reportes:
    - Productos. Mostrar en diferentes listados acorde a los criterios de su organización (consecutivo de código, almacén – código, etc.) los atributos de cada artículo registrado en el fichero maestro.
    - Saldos. Mostrar en diferentes listados acorde a los criterios de su organización (almacén, cuenta, etc.) los atributos de cada artículo registrado en el fichero maestro.
    - Histórico de movimientos.
    - Un producto y sus movimientos.
    - Submayor. En el que se debe mostrar todos los productos en existencia, detallando por cada uno, en cantidad e importe, el saldo inicial las operaciones y el saldo final, así como código, descripción, unidad de medida, documento y otros datos cualitativos captados que sean requerimientos de este reporte.
    - Productos ociosos.
    - Productos de lento movimiento, según los parámetros establecidos

- Conteo, con estructura de conteo a ciegas, del 100% y el 10%, aplicando en este último algoritmos definidos al efecto.

- Cierres

  De mes, condicionado a:

  - Transferencia al módulo de contabilidad de los comprobantes de operaciones que pudieran quedar pendientes.
  - Transferencia al módulo de cobros y pagos de las ventas y compras que pudieran quedar pendientes.

  De año, condicionado a:

  - Haberse hecho el cierre de mes.
  - Haber emitido y trasladado al módulo de contabilidad el comprobante de Operaciones de los saldos en cero para el correspondiente ajuste de importes.

MÓDULO DE COBROS Y PAGOS

Verificar en el Módulo de Cobros y Pagos los aspectos siguientes:

Procesos fundamentales que deben conformar este módulo:

- Apertura.
- Operaciones.
- Procesos contables.
- Informes.

- Apertura:

  En este proceso deben captarse todas las facturas de suministradores así como otros documentos que signifiquen obligaciones pendientes de pago y todas las facturas emitidas a clientes así como otros documentos que signifiquen derechos pendientes de cobro. El cierre de estas operaciones debe ser independiente y condicionado a su cuadre con los correspondientes saldos en el mayor.

- Operaciones. Debe incluir:

  Ventas, que sean registradas automáticamente transferidas del módulo de facturación o a través de captación por tecleo de las Facturas emitidas, con los siguientes datos:

  - Cliente.

- No. de factura (debe validarse el número consecutivo).
- Fecha de la factura.
- Fecha de cobro otorgada al cliente.
- Importe total.
- Importe pendiente.
- Contabilización.

Compras, que sean registradas a través de captación por tecleo de los documentos recibidos.

- Proveedor.
- Documento.
- Fecha.
- Importe total.
- Importe pendiente.
- Contabilización.

Cobros, pagos, liquidación de pagos y cobros anticipados, que en todos los casos sean registrados a través de captación por tecleo de los documentos recibidos.

- Cliente o Suministrador.
- Documento.
- Fecha.
- Importe total.
- Saldo por cobros y pagos parciales.
- Contabilización.
- Detalles de las facturas amparadas en el documento.

Transferencia a Efectos por Cobrar, con los mismos datos originales de la factura.

Transferencia de efectos por cobrar a cuentas por cobrar, manteniendo la fecha original de la factura para su inclusión correcta en el análisis por edades.

Debe confeccionarse un comprobante por cada tipo de operación del lote captado y trasladarse al módulo de contabilidad.

- Informes
  - Registro de operaciones. Se debe emitir un registro por tipo de operación de cada lote captado, con numeración consecutiva.
  - Análisis por edades. En el que debe mostrar por cada cliente o suministrador, según sea el caso, una relación de los documentos

pendientes de cobro o de pago analizados por el rango de edades predefinido. En caso de que la fecha de la factura y la del plazo dado al cliente para su cobro coincidan se toma la fecha de la factura, de no coincidir se toma la fecha del plazo al cliente.

- Submayores. Se debe emitir uno por cada concepto de derechos y obligaciones, analizado por sus cuentas asociadas, mostrando el saldo de cada deudor o acreedor, así como el reporte de cobros y pagos del período.

MÓDULO DE FACTURACIÓN

Verificar en el Módulo de Facturación los aspectos siguientes:

- Datos que debe contener la factura confeccionada automáticamente en la proforma establecida, a partir de la información primaria captada, además de la información de control característica de este tipo de documento:
  - Numeración consecutiva automática.
  - Definición de diferentes condiciones de pago.
  - Posibilidad de aplicarse distintos tipos de descuentos.
- Aspectos de control a tener en cuenta en el Módulo:
  - Registro de plazos para el cobro a los clientes.
  - Información de las fechas de vencimiento de los adeudos de los clientes.
  - Afectación a las correspondientes cuentas de inventario y clientes.
  - Imposibilidad de modificar facturas después de emitidas. Deben ser canceladas y emitidas de nuevo.
  - Posibilidad de trabajar basándose en órdenes de pedidos de clientes registradas previamente.
  - Posibilidad de modificar o anular pedidos.
- Informes:
  - Relación de los plazos para el cobro a los clientes.
  - Listado con las fechas de vencimiento de los adeudos de los clientes.
  - Relación de pedidos de cliente pendientes de cumplimentar.
  - Relación de facturas de clientes en un periodo.
  - Relación de facturas canceladas.

- Listados de las operaciones realizadas para cualquier periodo que se solicite.

MÓDULO DE ACTIVOS FIJOS TANGIBLES

Verificar en el módulo activos tangibles los aspectos siguientes:

Procesos fundamentales que deben conformar este módulo:

- Carga inicial.
- Operaciones.
- Movimientos.
- Posteo.
- Operaciones contables.
- Informes.

Las pantallas de las captaciones que se realicen en los distintos procesos deben contener todos los datos de referencia, control y cuantitativos, tanto de los activos fijos como de sus depreciaciones. También deben ser consideradas las características técnicas de cada activo:

- Carga inicial. En este proceso se registran los datos de los activos fijos existentes en la entidad al momento de comenzarse a trabajar con el módulo. El cierre de la misma solo debe tener efecto cuando los importes de los valores de los activos fijos captados y el de sus depreciaciones sean coincidentes con los respectivos saldos que muestre el mayor.
- Operaciones. En este proceso deben ser consideradas las actualizaciones de cualquiera de los conceptos que conforman el conjunto de datos que identifican a cada activo fijo.
- Movimientos. Este proceso debe contemplar el registro de todos los movimientos que sean inherentes a esta actividad.
- Unidades básicas y módulos de control. Esta modalidad en los activos fijos, por tener características específicas requiere que su operatoria se independice del resto de los Activos Fijos. En este proceso deben ser considerados su creación y tratamientos propios.
- Posteo. En este proceso debe ser realizado el traslado hacia el fichero maestro de los movimientos y actualizaciones efectuados.

- Operaciones Contables. En este proceso deben incluirse la depreciación, la elaboración de Comprobantes tanto de la depreciación como de cada uno de los conceptos que dieron lugar a los movimientos de activos fijos, el traslado al módulo de contabilidad de los comprobantes elaborados y el traslado al módulo de cobros y pagos de los cobros por ventas y los pagos por compras de activos fijos.
- Informes:
    - Activos Fijos totalmente depreciados.
    - Listado por áreas de responsabilidad, con totales de valor y depreciación por área y total general.
    - Submayor por activo fijo.
    - Reportes de altas y bajas.
    - Traslados de activos fijos (alquilados y enviados a reparar).
    - Revalorización (revaluación por avalúos).
    - Reparaciones Generales que incrementan el valor del activo.
    - Listado por consecutivo de número de inventario.
    - Saldos por cuenta – subcuenta.

    Cierres:

    - De mes. Tiene que estar condicionado a la ejecución del proceso de depreciación y que el número del próximo mes de operaciones sea el del mes actual más uno.
    - De año. Tiene que estar condicionado a que se haya efectuado el cierre del último mes del periodo fiscal. En este proceso debe hacerse el borrado de todos los movimientos efectuados en el año, previa salva, excepto los correspondientes a los activos fijos alquilados y a los mandados a reparar.

MÓDULO DE NÓMINAS

Verificar en el Módulo de Nóminas los aspectos siguientes:

Procesos fundamentales que deben conformar este Módulo:

- Carga.
- Operaciones de nóminas.
- Operaciones contables.
- Retenciones.
- Informes.

- Carga:

  Este proceso se ejecuta en la apertura del módulo y deber contener al menos la creación de los siguientes ficheros maestros:

  - Trabajadores.
  - Descuentos que no constituyen retenciones.
  - Retenciones, por tipo de retención y trabajador.
  - Contribución especial a la Seguridad Social.
  - Vacaciones.

- Operaciones de nómina. En este proceso los formatos de impresión de las nóminas deben incluir los requisitos de control que se exigen para estos documentos:

  a) Captación de los datos para la confección de las nóminas y nominillas. Se debe aplicar un mecanismo de cuadre que permita la detección de errores o fraudes.

  b) Cálculo automático de las nóminas y nominillas incluyendo el 9.09%, el impuesto por la Utilización de la fuerza de trabajo, de la contribución a la Seguridad Social y la aplicación, si procede, de las retenciones registradas en su fichero maestro. Los factores que se utilicen en los cálculos sean tomados de sus correspondientes ficheros maestros.

  c) Actualización automática del Submayor de vacaciones a partir del cálculo del 9.09% aplicado en las nóminas y nominillas de sueldos y jornales, y del tiempo a disfrutar registrado en la Nómina de Vacaciones.

  d) Confección y emisión de la nómina y nominilla de sueldo y sus comprobantes de Gastos y cobros.

  e) Confección y emisión de la nómina y nominilla de jornales y sus comprobantes de Gastos y cobros.

  f) Confección y emisión de la nómina y nominilla de vacaciones y subsidios y sus comprobantes correspondientes.

- Retenciones. En este proceso se incluyen:

  - Los ajustes efectuados a las retenciones.
  - Confección de comprobantes de los ajustes a las retenciones y de las retenciones aplicadas.
  - Listados de las retenciones y descuentos aplicadas y no aplicadas.
  - Confección de los comprobantes de operaciones correspondientes.

- Operaciones contables. Este proceso incluye:
    - Confección de un comprobante por cada tipo de nómina y nominilla.
    - Transferencia al módulo de contabilidad de los comprobantes confeccionados.
    - Transferencia de las retenciones a descontar al Módulo de cobros y pagos.
- Informes:

  a) Listado de alerta sobre trabajadores con más de 20 días acumulados

  b) Submayor de vacaciones en tiempo e importe.

ANEXO 2 - INDICACIONES PARA AUDITORÍA HACIENDO ÉNFASIS EN LA SEGURIDAD ASOCIADA A ESTOS SISTEMAS

POLÍTICAS SOBRE SEGURIDAD INFORMÁTICA

- Chequear que la administración en la entidad tenga una política, acorde a las regulaciones que rigen sobre la seguridad de la información que se procesa, intercambie, reproduzca o conservan a través de las tecnologías de información, y si tiene establecidos los mecanismos de control para garantizar el cumplimiento de las regulaciones previstas en su Reglamento.

- Verificar si la política a seguir para lograr la Seguridad Informática en la entidad, se ha hecho un análisis de la gestión informática, que abarca: su organización, flujo de la información, tecnologías de información disponibles, alcance de la actividad informática dentro y fuera de la entidad, categoría de clasificación de la información que se procesa, determinación de la información sensible para la actividad fundamental de la entidad y los controles establecidos; que brinden los elementos indispensables para evaluar la vulnerabilidad del sistema y los principales riesgos a que esté expuesto.

Plan de Seguridad Informática y de Contingencias

- Chequear que exista el Plan de Seguridad Informática que se instituye como una exigencia para todas las entidades, en el cual se reflejen las políticas, estructura de gestión y el sistema de medidas, para la Seguridad Informática, teniendo en cuenta los resultados obtenidos en los análisis de riesgos y vulnerabilidad realizados. El máximo dirigente de cada entidad garantiza, según corresponda a la actividad informática que se desarrolle, que se elabore, ponga en vigor, cumpla y actualice periódicamente

- Verificar que la aplicación de estos planes sea objeto de aprobación y control por parte de las distintas instancias de la propia entidad

- Verifique que existe el Plan de Contingencia para la Seguridad Informática, que contenga las medidas que permiten, en caso de desastres, la evacuación, preservación y traslado, de los medios y soportes destinados al procesamiento, intercambio y conservación de información clasificada o sensible. Así que contemple las medidas pertinentes para la conservación y custodia de los ficheros creados con fines de salvaguarda.

SEGURIDAD FÍSICA

Requerimientos de protección física

- Chequear si en las áreas reservadas aquellas donde la información que se procesa, intercambia, reproduce y conserva a través de las tecnologías de información sea sensible para la entidad, se aplican las normas de protección establecidas de acuerdo a las características de cada lugar.

- Chequear si la entrada o permanencia de las personas en las áreas reservadas es controlada, requiriéndose la autorización expresa de la persona facultada para ello. En el caso del personal de servicio, mantenimiento de equipos u otro que eventualmente

precise permanecer en el área lo hará siempre en presencia de las personas responsables.

- Chequear que los soportes pertenecientes a una entidad, cuando contengan información sensible, sean controlados, debiendo reflejar los datos de control en los soportes removibles que lo permitan, señalizándolos de forma clara y visible.

- Comprobar que la utilización de los soportes de propiedad personal o de otra entidad, cuentan con la autorización del jefe administrativo del lugar, si se aplican los controles establecidos en los casos en que la información contenida en los mismos sea clasificada o sensible.

- Revisar los soportes si el traslado de los mismos se realiza respetando las normas de conservación de los mismos, con el objetivo de garantizar la integridad y confidencialidad de la información que contienen y cumplirán las medidas de protección establecidas de acuerdo a la categoría de clasificación de la misma.

- Chequear el uso del Libro de Incidencias para las áreas donde se utilicen las tecnologías informáticas, donde se anotarán todos aquellos eventos que revistan un interés especial , tales como, roturas, mantenimientos, traslados, uso de estas tecnologías por personal ajeno a la entidad, aparición de virus informáticos.

- Chequear que todos los locales con tecnologías informáticas deberán tener los tomacorrientes señalizado el voltaje a que trabajan o suministran.

- Verifique que se protege por medios técnicos a los programas y sistemas informáticos que no requieren actualización periódica, así como se garantiza que los soportes tecnológicos de información que contienen las salvas de los programas y sistemas, estén también protegidos físicamente contra escritura.

- Chequear que las salvas se conserven en la entidad y en al menos otro lugar distante a la misma, que cumpla con las condiciones técnicas y seguridad necesarias, para evitar su destrucción en caso de accidentes.

- Chequear si se garantiza la climatización y/o ventilación especificada por el fabricante de las tecnologías informáticas, así como el cumplimiento del mantenimiento periódico de las mismas.

- Las tecnologías informáticas fundamentales para la operación de sistemas informáticos, tales como los servidores, deberán estar conectados a fuentes de respaldo de energía y éstas deberán poseer limitadores de voltaje.

SEGURIDAD LÓGICA

- Verifique que las tecnologías de información en que se procese, intercambie, reproduzca y conserve información sensible, se les implementen mecanismos para identificar y autenticar los usuarios.

- Verificar que sean implementados mecanismos de control que permitan controlar la traza o el registro de los principales eventos que se ejecuten y puedan ser de interés para la detección o esclarecimiento ante violaciones de la Seguridad Informática.

- Verifique que las aplicaciones destinadas al procesamiento de información clasificada o sensible, reúnan los requisitos siguientes:

  a) incluyan claramente documentadas las políticas de acceso ;

  b) marcar los objetos con los distintos niveles de clasificación de la información que permita la aplicación del control

  c) contar con la capacidad de registrar todas las operaciones principales, realizadas en el tratamiento de bases de datos.

- Chequear si existe protección contra ataques o alteraciones no autorizadas, a los mecanismos de seguridad técnica que se apliquen, tanto a nivel de sistema operativo como de aplicaciones.

- Chequear si se tienen las salvas actualizadas de las informaciones, con el fin de recuperarlas o restaurarlas en los casos de pérdida, destrucción o modificación mal intencionado o fortuito, de acuerdo a la clasificación o importancia de la información que protegen.

- Verificar en dependencia de las características técnicas de los equipos si se aplican detectores automatizados de violaciones, que permitan conocer y neutralizar las acciones que constituyan un riesgo para la confidencialidad, integridad y disponibilidad de la información.

- En las tecnologías de información en que se procesa información clasificada o sensible, se aplicarán mecanismos de protección que controlen el acceso a través de dispositivos a los soportes removibles.

SEGURIDAD DE OPERACIONES

- Toda entidad tiene que mantener identificadas las tecnologías de información que posean.

- Chequear que no se usen, distribuyan o comercialicen de herramientas de Seguridad Informática que no cuenten con la aprobación del órgano correspondiente del Ministerio de Informática.

- Chequear que la entidad esta obligada a implementar medidas de protección contra virus informáticos, en correspondencia con sus condiciones específicas. así como aplicar las medidas básicas.

RESPONSABLE DE LA SEGURIDAD INFORMATICA Y ADMINISTRADOR DE RED

- Chequear que para las tecnologías de información instaladas haya designado un responsable para la atención de la Seguridad Informática en las diferentes áreas de trabajo cumpliendo sus funciones

- Verificar que la entidad cuenta con la existencia de un Administrador de red que cumple con sus funciones básicas.

TRABAJO EN REDES

Seguridad de operaciones en el ambiente de las redes de datos.

- Verifique si hay implementado los mecanismos de seguridad en las redes de datos; así como de aquellos que permitan filtrar o depurar la información que se intercambie, de acuerdo a los intereses predeterminados por cada una de ellas.

GLOSARIO

Manual de Usuario: Contiene una explicación detallada y de fácil comprensión de cada opción y proceso, haciéndose hincapié de cómo operarlos y de las acciones a tomar ante las diferentes alternativas que se presenten.

Manual de Explotación: Contiene una completa explicación del funcionamiento del Sistema incluidas todas las interrelaciones entre los procesos y las estructuras de las bases de datos.

LEGISLACIÓN DE CONSULTA Y REFERENCIA

- **Resolución 6/96 del MININT**. “Reglamento sobre seguridad Informática”.
- **Decreto Ley 199/99 del Consejo de Estado** “Sobre la seguridad y Protección de la Información Oficial”.
- **Resolución 188/2001 del MIC**. ”Metodología para el acceso de las entidades cubanas a Internet o a otras redes de datos externas a las mismas.”

- **Resolución 297/03 MFP**. “Definiciones de Control Interno. Contenido de los Componentes y sus Normas”.
- **Resolución 65/03 MIC**. “Sobre inscripción de red Privada de Datos”.
- **Resolución conjunta MFP-MIC/2004** “Requisitos para los sistemas contables financieros”.
- **Resolución No. 340/04 MFP** “Procedimientos para dictaminar sobre el grado de adaptación a las Normas Contables Cubanas de los Sistemas Contables – Financieros soportados sobre las tecnologías de la información”.
- **Resolución 12/2005 MIC**. “Requisitos adicionales para los sistemas contables soportados sobre las tecnologías de la Información”.
- **Acuerdo 6058 CECM** (09-07-07) Lineamientos para el Perfeccionamiento de la seguridad de las Técnicas de la Información en el país.
- **Resolución 127/07 del MIC**. “Reglamento sobre la Protección y seguridad técnica de los sistemas informáticos”.

Anexo No. 5

Seguridad de las Aplicaciones y Bases de Datos					
5.7	¿Se encuentran los programas fuentes en la misma ubicación donde se ejecuta el programa compilado?	Art. 42			
5.7	¿Existen manuales y/o procedimientos de seguridad para las aplicaciones informáticas?	Art. 43			
	¿Está habilitado algún método de identificación y autenticación de los usuarios para acceder a la aplicación y la base de datos?	Art. 45			
	¿Los programas, bases de datos y ficheros que conforman el sistema están instalados en el disco duro de la computadora, en un directorio con acceso restringido solamente a los usuarios autorizados?	Art. 48			
	¿Son los usuarios autorizados los que tienen acceso a las aplicaciones y bases de datos?	Art. 48			
	¿Está habilitada la opción de auditoría para las bases de datos?	Art. 48 y 58			
	¿Tienen los usuarios los permisos y derechos correctos sobre las bases de datos, atendiendo el cargo y funciones que desempeñan?	Art. 42 y 48			
	¿La información contenida en el fichero de palabras claves se encuentra cifrada, de forma tal que al editar el contenido del mismo no puedan conocerse las claves asignadas?	Art. 47 inc e)			
	¿Las claves de acceso de administración del sistema son de uso exclusivo del personal en funciones de administración?	Art. 48			
	¿Existe un documento escrito que defina los niveles de acceso de los usuarios, roles asignados y está aprobado por el jefe inmediato?	Art. 48			
	¿El acceso para la manipulación, modificación o edición de las bases de datos se logra solamente a partir de las opciones que brinda para ello el propio sistema?	Art. 48			
	Obtener las cuentas creadas en el sistema informático y realizar el análisis en busca de: – Obtener las cuentas creadas y sus roles de accesos, analizando su correspondencia con el cargo que ocupan.	Art. 47 Art. 42			

	– Cuentas de usuarios pertenecientes a trabajadores que cesaron sus relaciones laborales. – Si tienen definido el tiempo de expiración de las cuentas. – Si todas las cuentas tienen password asignadas. – Si cada usuario tiene una password personal (no se comparten). – Si tienen definida la longitud mínima de la password y no menor de 6 caracteres	Art. 46 Art. 47 inc c)			
	¿La aplicación cuenta con procedimientos programados (Trazas) que permitan conocer la ocasión en que las personas autorizadas hacen uso de la misma y las funciones que emplean?	Art. 43			
	¿Desde el sistema se posibilita la realización de salvas de la información?	Art. 53			
	¿Existe una copia de seguridad de los programas fuentes de la aplicación, la que se encuentra guardada fuera del área o local donde se encuentra instalado el sistema informático?	Art. 54			
	¿Se realizan restauraciones de las salvas con regularidad para asegurar el funcionamiento adecuado del proceso de Backup y restauración? ❖ ¿Se encuentran los Backup en las ubicaciones definidas para esos efectos (ubicación física y lógica de la información? ❖ ¿Se tienen documentados los Backup realizados, responsables, fechas de realización y su estado?	Art. 53 y 54			
	¿Las trazas de los eventos realizados sobre las bases de datos se encuentran habilitadas y garantizan su conservación por un período mínimo de un año? ❖ En base de datos (BD) SQL, abrir la consola de administración SQL SERVER, entonces se escoge la BD a analizar, damos clik derecho y escogemos propiedades; entonces en la pestaña que dice Transaction Log verificar el tamaño del fichero y su ubicación.	Art. 58			
	¿Se tiene delimitado las funciones de desarrollo, prueba y producción de Software?	Art. 42 y 43			

	Consideramos que deben incorporarse estos puntos a controlar en aquellas entidades donde diseñan Softwares u otras aplicaciones específicas (DESOFT, SEGURMATICA, UCI, Universidades, étc): a) ¿Se definen y documentan los procesos establecidos para transferir el software del ambiente de desarrollo al de producción? b) ¿El software de desarrollo y el de producción se encuentran funcioando en computadoras diferentes? c) ¿Los compiladores, editores y otras herramientas de desarrollo o utilidades del sistema son accedidas solamente por los usuarios pertenecientes al área de desarrollo? d) ¿Se tienen definidos perfiles de usuario diferentes para los sistemas en producción y de prueba? e) ¿En las pruebas del sistema no se aplican informaciones sensibles de una entidad? f) ¿Se tiene definido un proceso de cuarentena para someter los sistemas a pruebas? ¿En las pruebas se comprueba la disponibilidad del sistema, seguridad, efectos sobre otros sistemas y facilidades del usuario? g) ¿Existe un registro de auditoría para el control de las actualizaciones de los programas en producción? h) ¿Se conserva la versión anterior del Software de aplicación como una medida de contingencia?				
	¿Existe un procedimiento escrito donde se detallen los pasos a seguir para la recuperación de las aplicaciones y bases de datos ante la ocurrencia de fallas o desastres?	Art. 87			

Anexo No. 6

Manual del MAC

Exploración

Además, debe precisar el grado de automatización y el nivel de actualización tecnológica, enfatizando en:

- Políticas y normas informáticas.
- Programa de informatización de la entidad.
- Esquema y ubicación de las áreas automatizadas y su personal.
- Nivel tecnológico alcanzado y planes de informatización.
- Inventario de recursos informáticos.
- Documentación de sistemas, planes de trabajo y plan de seguridad.

Controles generales

Controles a los recursos físicos.

Si se excluyen las causas de riesgos extraordinarias como guerras, catástrofes naturales, etc. que exigen un tratamiento adecuado a sus magnitudes, las causas de riesgos habituales que se presentan son: daños y destrucción de los sistemas de información, fallas de los equipos y líneas de transmisión.

Los controles que se apliquen deben ser preventivos, de detección y correctivos, y se contemplan en el plan de medidas de seguridad.

- **Controles preventivos:** Son diseñados para disminuir la probabilidad de que se produzcan errores, omisiones o fraudes.
- **Controles correctivos:** Son procedimientos de chequeo que corrigen errores u omisiones una vez que estos son detectados.
- **Controles de detección:** Son los que detectan e informan que se han presentado causas de riesgos.

Los puntos que debe proteger este plan se relacionan con el acceso a tecnologías de la información (robo o destrucción de recursos materiales, servicios o informaciones), fuego, inundaciones, fallos de energía, clima, etc.

El auditor verificará si existen equipos sin instalar y tiempo que llevan en esas condiciones, reportes de mantenimiento para determinar la frecuencia de errores inducidos por problemas de hardware y la confiabilidad de éste, así como las medidas necesarias para proteger contra fluctuaciones o interrupciones de la energía, etc.

Controles a los recursos lógicos

Se denominan controles lógicos de acceso a las medidas de seguridad implementadas a través de medios informáticos, utilizadas para restringir el acceso a los sistemas. La implementación de estos controles permite restringir el acceso de acuerdo con los requerimientos de procesamiento de los usuarios de la organización (quién puede acceder a qué datos) indicando el tipo de acceso permitido.

Existen varios criterios que pueden aplicarse para la determinación de los permisos de acceso:

- Identificación.
- Roles (como programador, líder de proyecto, administrador del sistema, etc.).
- Ubicación.
- Horario.
- Transacciones.
- Segregación de funciones.
- Modalidad de acceso.

Existen varios métodos para proveer control de acceso local y remoto, los que se diferencian significativamente en términos de precisión, sofisticación y costo. Estos métodos no son excluyentes y usualmente se utilizan en forma combinada.

Controles de acceso interno

- Palabra clave.
- Encriptación.
- Listas de control de acceso.
- Límites sobre la interfase de usuario.
- Etiquetas de seguridad

Controles de acceso externo

- Dispositivos de control de puertos.
- "Firewalls" o puertas de seguridad.

Administración de los controles de acceso

Una vez establecidos el control de acceso sobre sistemas y aplicaciones, es necesario realizar una eficiente administración de la seguridad lógica, lo que involucra la implementación, seguimiento, pruebas y modificación sobre el acceso de los usuarios a los sistemas. Existen tres enfoques básicos para realizar la administración del control de acceso:

- **Administración centralizada:** Existe una función responsable de configurar el control de acceso.
- **Administración descentralizada:** En este caso los usuarios de los medios informáticos controlan el acceso directamente.
- **Administración híbrida:** Combina la administración centralizada y descentralizada.

La información puede ser:

- **Pública:** Puede ser visualizada por cualquier persona que acceda al ambiente de trabajo informático.
- **Restringida:** Puede ser visualizada solamente por un grupo que normalmente trabaja con la información.
- **Clasificada:** Requiere medidas de seguridad estrictas tendentes a evitar su exposición a personal no autorizado.

Estos diversos tipos de información requieren diferentes medidas de seguridad:

- La información pública debe restringirse a individuos específicos.
- La información restringida debe almacenarse de manera segura y protegida.
- La información clasificada deber ser restringida, encriptada y el acceso requerir un proceso de entrada en el sistema.

Encriptación: Importante herramienta para la protección de la información en diversos aspectos como confidencialidad, integridad, firma electrónica y técnicas avanzadas. Se basa en dos componentes básicos: un algoritmo y una clave. Básicamente existen dos tipos de sistemas de encriptación: sistemas de claves asimétricas (pública y privada) y sistemas de clave simétrica.

Firma electrónica: La documentación electrónica permite su rápido procesamiento y transmisión, y aumenta la eficiencia al disminuir la dependencia del papel.

La autenticidad de un documento en papel, tradicionalmente se basaba en la firma del autor. Para que sea posible aprovechar las ventajas de la documentación electrónica, resulta necesario contar con el equivalente electrónico de la firma, para asegurar la autenticidad de esta documentación.

La encriptación facilita establecer vínculos unívocos que permitan identificar a personas determinadas, al igual que la firma de cada individuo, además de proteger la integridad de los datos,.

Para la implementación de un sistema de encriptación es necesario tener en cuenta las siguientes consideraciones:

- Establecer estándares de implementación y diseño.
- Decidir la implementación sobre software o hardware.
- Definir el algoritmo y la administración de las claves.
- Establecer la seguridad sobre los módulos de encriptación.
- Definir la aplicación de la encriptación sobre las redes de comunicaciones.

Estas definiciones deben estar adecuadamente documentadas.

Controles de organización

Se verificará la estructura organizativa para valorar la ubicación de las áreas automatizadas y su integración, la segregación de funciones para determinar las responsabilidades del personal, restricciones de acceso por niveles a programas, ficheros y documentación. Se deben revisar las normativas y procedimientos sobre responsabilidad por el control.

Controles de seguridad

- Verificará el control de acceso físico y lógico a los locales, los equipos, aplicaciones y la documentación de autorización.
- Comprobará el cumplimiento de las normativas y orientaciones recibidas por las instancias y comprobará la existencia de antivirus y su actualización.
- Revisará la existencia del plan de seguridad informática y contra contingencias, su adecuación, suficiencia y cumplimiento. En caso de no estar elaborado se debe realizar un análisis de los riesgos.

Controles específicos

- **Control de acceso:** Verificar el acceso mediante claves secretas a las aplicaciones y las opciones susceptibles a violaciones y fraudes, así como la asignación de las palabras claves por el máximo dirigente del área, la confiabilidad y privacidad de las mismas.
- **Controles de entrada de datos:** Verificar la autorización, preparación y transmisión de la información así como la validación automatizada de los datos.
- **Controles de procesamiento:** Verificar que existen rutinas que comprueban internamente las operaciones susceptibles de ser alteradas y que se puedan restaurar transacciones interrumpidas bruscamente.

- **Controles de salida:** Verificar que los reportes o listados cumplan con los requisitos mínimos establecidos y entregados oportunamente.

Controles para aplicaciones que se soportan sobre redes:

Verificar:

- Las políticas de control de acceso físico y lógico a las terminales y los servidores de la Red.
- La seguridad y efectividad de todos los componentes de la red.
- Las documentaciones técnicas, estructura y organización.
- La administración de la red por personal calificado.

Anexo No. 7

GUÍA DE CONTROL

Resolución No.127/07 del MIC sobre la Seguridad Informática

No	Aspectos a Verificar	SÍ	NO	NP
	SISTEMA DE SEGURIDAD INFORMATICA			
27.	Se encuentra diseñado, implantado y actualizado un Sistema de Seguridad Informática. (Art.4 y 7)			
28.	Para la confección del Plan de Seguridad Informática (PSI) se utilizó la Metodología de la OSRI/MIC. (Art. 6)			
29.	La entidad posee especialistas en Seguridad Informática. (Art.6 y 8)			
30.	Está determinado en nivel de acceso de los usuarios a los bienes informáticos. (Art. 9a)			
31.	Se ha especificado al personal las medidas y procedimientos de seguridad. (Art. 9d)			
32.	Se imponen o proponen sanciones ante violaciones de seguridad. Art. 9f)			
33.	Se establecen controles que impiden la instalación de SW y HW sin la debida autorización. (Art. 10e, 43, 64)			
34.	Posen los usuarios de Tecnologías Informáticas (TI) preparación necesaria sobre Seguridad Informática. (Art. 12a, 65)			
	CLASIFICACIÓN Y CONTROL DE LOS BIENES			
35.	Los bienes informáticos de la entidad son utilizados en funciones de trabajo en correspondencia con su objeto social. (Art. 13)			
36.	Se posee un inventario de los bienes informáticos incluyendo sus componentes y sus especificaciones técnicas. (Art. 14)			
37.	Cada bien informático se encuentra bajo custodia documentada de una persona. (Art. 15)			
38.	Se controla el movimiento de los medios informáticos. (Art.16, 41)			
	DEL PERSONAL			
39.	Se encuentra incluida como responsabilidad laboral del personal su responsabilidad en la seguridad informática. (Art. 17)			
40.	Los contratos de empleo del personal especifican la vigencia de la responsabilidad del trabajador ante la seguridad informática aún cuando finalice su relación laboral. (Art. 19)			
41.	La entidad ejecuta control dl empleo de las TI. (Art. 22)			
42.	Se controla el uso de programas que comprometen o monitorean la seguridad del sistema informativo o procesan información			

No	Aspectos a Verificar	SÍ	NO	NP
	contrarias al interés social. (Art. 26)			
No	Aspectos a Verificar	SÍ	NO	NP
	SEGURIDAD FISICA Y AMBIENTAL			
17.	Las TI que poseen información de valor están debidamente protegidas. (Art. 27, 29 a , 30, 31, 32, 33)			
18.	Las TI están protegidas contra alteraciones, sustracciones, de estas o sus componentes (sellos de seguridad). (Art. 36)			
19.	Están separados y protegidos los cables de información (datos) de los de alimentación (voltaje). (Art. 37)			
20.	Tienen la TI implantado un plan de mantenimiento preventivo. (Art. 38)			
21.	Están autorizados debidamente los medios técnicos que por necesidad de la entidad o tipo de labor a ejecutar salen de la misma. (Art. 39)			
22.	Se evita mediante control y procedimientos adecuados la salida de información que poseen las TI que causan baja, salen a reparación o se trasladan de función. (Art. 40)			
	SEGURIDAD DE OPERACIONES			
23.	Se atiende el principio de separación de funciones sobre tareas que no deben ejecutarse por una misma persona. (Art. 42)			
24.	Están controladas y se poseen prueba documental las acciones ejecutadas para cubrir brechas de seguridad y corrección de errores del sistema. (Art. 44)			
	IDENTIFICACION, AUTENTICACION Y CONTROL DE ACCESO			
25.	Está claramente definido el control de acceso de usuarios a los sistemas. (Art. 45)			
26.	Los accesos de usuarios son autorizados por el jefe inmediato de estos así como su desactivación en caso de baja de los mismos. (Art. 46)			
27.	La estructura, fortaleza y frecuencia de cambio de contraseñas están en función del riesgo estimado para el acceso que se protege. (Art. 47)			
28.	Las contraseñas combinan números, letras, sin significado evidente con longitud mínima de 6 caracteres. (Art. 47c)			
29.	Se encuentra implantado procedimiento escrito que otorga o suspende derecho de acceso a sistemas y datos para cada usuario. (Art. 48)			
	SEGURIDAD ANTE PROGRAMAS MALIGNOS			
30.	Las TI se encuentran protegidas con programas antivirus. (Art. 50)			

31.	Los antivirus utilizados están debidamente aprobados en el país y están actualizados. (Art. 50)			
	RESPALDO DE LA INFORMACION			
32.	Está implementado un sistema fiable de respaldo. (Art. 53)			
33.	Los respaldos, con los informes de las copias y los procedimientos de recuperación son almacenados en otra ubicación diferente al origen. (Art. 54)			

34.	Los respaldos mantienen las mismas condiciones ambientales que el origen. (Art. 55)			
35.	Se prueban regularmente los respaldos de información para verificar su estado y uso ante emergencias. (Art. 56)			
	SEGURIDAD EN REDES			
36.	Se encuentran implementados mecanismos de seguridad de redes. (Art. 57)			
37.	Están habilitadas las opciones de seguridad con que cuentan los Sistemas Operativos que garantizan la protección de los servidores y terminales, el acceso a la información, el monitoreo y auditoria de los principales eventos por un tiempo no menor de 1 año. (Art. 58)			
38.	Los productos de fiscalización y monitoreo instalados son los autorizados en el país. (Art. 59)			
39.	La arquitectura y configuración de los componentes de seguridad de la red y la implementación de los servicios que presta, están en correspondencia con las políticas definidas y aprobadas para su empleo, no dejándose a la iniciativa de una persona. (Art. 60)			
40.	La red cuenta con un Administrador para su operación. (Art. 61)			
41.	Cumple el administrador de red las obligaciones relacionadas con la Seguridad Informática. (Art. 62)			
42.	Se tiene prohibida la administración de redes mediante conexiones conmutadas de redes públicas. (Art. 63)			
43.	Están establecidas barreras de protección para conexiones desde o hacia el exterior de la entidad. (Art. 66)			
44.	Se tienen instrumentados y ejecutan procedimientos periódicos de verificación de seguridad de las redes que detecten posibles vulnerabilidades. (Art. 67)			
45.	Las informaciones colocadas en servidores para su acceso público tienen procedimentado medidas que garanticen integridad y disponibilidad en correspondencia con los intereses de la entidad y el país. (Art. 70)			

46.	Si un sitio se encuentra hospedado en un servidor en el extranjero, este es réplica o espejo del sitio principal del ubicado en Cuba, con medidas de seguridad durante su actualización. (Art. 71)			
47.	Se prohíbe colocar sitios o páginas Web desde entidades estatales en servidores en el extranjero que ofrecen estos servicios de forma gratuita. (Art. 72)			
48.	Los servidores destinados al uso de la red interna no contienen servidores destinados a facilitar accesos hacia o desde el exterior. (Art. 73)			
49.	La red corporativa que provee servicios internos los realiza por puertos identificados y con dispositivos de protección que garantizan el acceso a los servicios por personal autorizado. (Art.74)			
50.	Las conexiones externas de la red se utilizan en interés de la entidad. Las cuentas de estos usuarios están aprobadas por la dirección de la entidad. (Art. 75)			
51.	Está establecida la prohibición de habilitar cuentas de correos electrónicos desde la entidad en servidores que se encuentran en el exterior del país. Si existen están justificadas y autorizadas por la dirección, especificándose el tipo de información a transmitir y plazo de vigencia. (Art. 76)			
52.	Está establecida la prohibición de vincular cuentas de correo electrónico de un servidor de la entidad a un servidor en el exterior con el fin de redireccionarla y acceder a mensajes. (Art. 77)			
53.	Las listas de correos y los chat se encuentran autorizados en todos los casos por la dirección de la entidad. (Art. 78)			
54.	Está establecida la prohibición a través de la red, la transmisión de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas o lesione la seguridad nacional. Se cuenta con controles que lo detectan, informándose a las instancias pertinentes. (art. 79)			
55.	Se controla el envío de correos no solicitados a múltiples (spam) cualquier sea su carácter. (Art. 80)			
56.	Se toman las medidas requeridas para impedir la sobrecarga de los canales de comunicaciones, restringiendo el envío/recepción de gran volumen de información y generación de mensajes a múltiples destinatarios. (Art. 81)			
57.	Se tienen implementados controles dirigidos a impedir e interrumpir la generación de cadenas y el envío de mensajes de correos de forma masiva a través de la red. (Art. 82)			
58.	Los usuarios con conexiones remotas autorizadas conocen de sus obligaciones al usar este servicio. (Art. 83)			

59.	Está establecida la prohibición de exploración o monitoreo de redes públicas en busca de vulnerabilidades o información de usuarios. (Art. 84)			
	INCIDENTES DE SEGURIDAD			
60.	Se encuentra establecida la estrategia ante incidentes o violación de la seguridad informática y bienes que se posee. Se incluyen alternativas para garantizar este servicio consecuente con los objetivos básicos de la entidad. (Art. 86)			
61.	Existen medidas y procedimientos para llevar adelante la estrategia ante incidentes que garanticen continuidad, restablecimiento y recuperación de los procesos informáticos. (Art. 87)			
62.	Las medidas y procedimientos de recuperación responden a la identificación de eventos (riesgos) que causan interrupción o afectación de los procesos informáticos. Se incluyen los responsables de su cumplimiento y los recursos necesarios. (Art. 88)			
63.	Los procedimientos definidos para la gestión de incidentes o violación de la seguridad informática siguen los pasos establecidos para su correcta evaluación. (Art. 89)			
64.	Ante cualquier incidente que afecte la seguridad informática se tiene establecido crear la comisión para esclarecer los hechos y establecer las medidas que eviten recurrencia. (Art. 90)			
65.	Está establecida la comunicación a la OSRI ante cualquier evento en contra de la seguridad informática y las instancias superiores de la entidad cumpliéndose con los datos establecidos en un reporte. (Art. 91)			
	PRESTACION DE SERVICOS A TERCEROS			
66.	En caso de prestar servicios informáticos a terceros se cuenta con la autorización emitida por la OSRI. (Art. 92)			
	INSPECCION A LA SEGURIDAD DE LAS TI			
67.	Se cumple que la inspección estatal en materia de seguridad a las TI es atribución del MIC, por lo cual la entidad no las realiza. (Art. 95)			
68.	El jefe de la entidad ha facultado bajo documento la realización de controles en materia de seguridad informática a las entidades subordinadas. (Art. 96)			
	TOTAL			

Anexo No. 8

Recomendaciones metodológicas para la aplicación de la guía propuesta

INTRODUCCION

La guía pretende lograr que al menos un mínimo de aspectos sea evaluado en las Auditorías Informáticas.

Por otra parte hay tópicos incluidos en el marco de la Auditoría Informática que no están reflejados en la presente guía pues en la generalidad se realizan como auditorías informáticas especializadas. Tal es el caso de la auditoría a aplicaciones.

Por otra parte, hay aspectos que pueden incluirse o en los que puede profundizarse en mayor o menor grado a partir de los objetivos que se definan de cada auditoría, de los resultados de la evaluación de riesgos, de los hallazgos y antecedentes y los temas en los cuales se decida profundizar, así como las pruebas, cuestionarios y otras herramientas a aplicar.

DE LA ENTIDAD AUDITADA

Obtener o actualizar información respecto a la entidad auditada que permita al auditor proyectar su trabajo. Como mínimo la referida a:

· Estructura orgánica

· Misión objetivos de trabajo y proyección

· Hardware de que disponen (descripción)

Para llegar a este nivel del detalle el auditor deberá solicitar los expedientes técnicos de cada una de las computadoras de la entidad, y el listado de todos los activos fijos informáticos.

· Existencia de redes, plataforma de trabajo (este aspecto se refiere al tipo de sistema operativo que tiene implementado la entidad Windows o Linux)

· Facilidades de Correo Electrónico y Comunicaciones en General existentes

· Entorno y ambiente informático

· Cultura informática de directivos y usuarios finales

· Aspectos organizativos

· Preparación técnica del personal implicado en las distintas actividades vinculadas con la informática

· Existencia de estrategia y proyección en materia Informática y Comunicaciones y su relación con los objetivos y proyección general de la entidad en si misma.

· Aplicaciones en explotación o en proceso de implantación

· Flujo de información

· Cambios en la tecnología que puedan ser representativos.

. Resoluciones internas que se relacionen con la actividad informática.

· Otros aspectos de interés, teniendo en cuenta los objetivos de la auditoría

· Políticas para adquirir tecnologías de información y comunicaciones, incluyendo software base y de aplicación.

Lo anterior aportará elementos con el objetivo de definir en que aspectos, incluidos o no en la presente guía que deberá enfatizar.

EVALUACION DE RIESGOS

Al realizar una auditoría informática es necesario hacer, sino un análisis minucioso de riesgos, al menos una apreciación de los mismos y a partir de ahí diseñar la auditoría. Este aspecto debe estar incluido en la fase exploratoria, lo cual permitirá durante el desarrollo de la auditoría una correcta evaluación de los controles.

La entidad auditada debe tener un sistema de controles y medidas basados en los posibles riesgos y causas de riesgos determinadas a partir de, los objetivos y metas de la entidad, riesgos del negocio y su relación con los TI y los riesgos asociados a las mismas. También debe tenerse en cuenta la probabilidad de ocurrencia de esos riesgos y el impacto que pueda causar la ocurrencia de los mismos para la organización, considerando la misión y objetivos de la misma y por ende no considerando aquellos, que sobre la base de ese análisis y de la evaluación costo-beneficio realizada, haya decidido asumir.

El auditor deberá evaluar:

· Si el sistema de controles y medidas es efectivo en relación con los riesgos y causas de riesgos considerados.

· Si hay riesgos y causas de riesgos que debieron ser considerados y no están presentes.

· En que medida se cumplen los controles y medidas que están definidos y en que documentos y procedimientos están establecidos.

Si el auditor detecta que no se ha realizado un trabajo en este sentido. Es decir si el auditado no tiene al menos definido:

1. ¿Qué riesgos se ha considerado pueden amenazar sus objetivos y los recursos asociados?

2. ¿Cuáles pudieran ser las causas de esos riesgos?

3. ¿Qué ha decidido asumir?

4. ¿Qué sistema de controles y medidas ha establecido y donde se encuentran reflejados?

Ello demuestra que no se ha hecho este análisis y el auditor deberá recomendar en el informe resultante la realización del mismo y evaluar el último aspecto a partir de la evaluación que pueda realizar por sí mismo de los tres primeros.

En tal sentido le será de gran ayuda la información relativa a la entidad auditada referida en el inciso II.

Al evaluar los riesgos, los controles y medidas definidos hay que tener en cuenta el impacto que puede tener el riesgo. Analizando, por ejemplo:

· Si hay muchas PC afectadas

· Si está involucrada información clasificada o sensible

· Si los efectos pueden trascender el marco de la entidad

· Cual es el daño potencial

· Probabilidad de ocurrencia

· Tiempo estimado de su neutralización

· Si puede afectar el prestigio y la imagen de la organización

· Nivel de afectación de los resultados económicos de la organización

· Si compromete el nivel de competitividad

· Si compromete la continuidad de los procesos y si esos procesos son clave

· Vinculación con posibles hechos delictivos

· Implicación político social

· Nivel de afectación a los objetivos de la entidad auditada

La relación no es biunívoca, es decir a un riesgo no tiene porque corresponder a una y sólo una causa de riesgo y viceversa.

Ej:

RIESGOS	CAUSAS
Pérdida de Información	Falta de preparación del personal
	Condiciones de las áreas Ej.
	Carencia de estabilizadores de

voltaje

Problemas con la salva de información

.....

Deficiente control de acceso

- Afectación del Servicio
- Fraude
- ..... Deficiente Control de Acceso
- Afectación de la Integridad de la Información

Se trata de evaluar si el sistema de medidas y control aplicados es efectivo es decir si actúa efectivamente sobre la(s) causa(s. Este análisis es clave en aquellos riesgos cuya ocurrencia produce un impacto considerable en la entidad.

A continuación una relación de riesgos y causas de riesgos frecuentes en la actividad informática a modo de ilustración:

RIESGOS

· Afectación a la integridad o disponibilidad de la información
· Ataque de programas malignos
· Entrada no autorizada a la red
· Afectación a la integridad de la información (datos y sistema)
· Pérdida de información
· Fraude, robo
· Divulgación de información secreta o de acceso "limitada"
· Afectaciones del fluido eléctrico
· Modificación no autorizada del software o bases de datos que soportan información

contable.

· Que el receptor del mensaje o la información no sea el destinatario original

· Que el emisor no sea quien dice o debe ser

· Que se modifique el mensaje o la información original

· Otros riesgos (tener en cuenta las características actuales de la entidad auditada y su sistema informático, tener en cuenta los riesgos provenientes de fuentes internas y externas así como los correspondientes a las distintas áreas y/o actividades de la entidad objeto de estudio)

CAUSAS DE RIESGOS

- Fallas en el procedimiento y ejecución del mantenimiento y la documentación del soft

· Relativas a la organización de la administración de las TIC de la aplicación, de la red

· Roturas

· Errores en la manipulación del software base y de aplicación

· Hackers

· Crackers

· Desastres naturales (temblores de tierra, ciclón, inundaciones, etc.)

· Accidentes (incendio, derrumbe, etc)

· Relativas a la elaboración, control y actualización de PSI y PC

· Falta de cultura informática y preparación de directivos y personal implicado en los sistemas de información

· Incumplimientos relativos a la disciplina y Organización del Trabajo Informático

· Inadecuado procedimiento de salva y respaldo o inexistencia de los mismos

· Ausencia de plan de mantenimiento de las salvas o indisciplina en su ejecución

· Relativas al procedimiento asociados al cambio de personal (informático y usuario final)

· Deficientes normas y procedimientos para el control de acceso a la información o inexistencia de los mismos

· Fisuras de Seguridad de las TIC

· Relativas a deficiente selección del personal

· Relativas a la preparación y adiestramiento del personal

· Deficiente puntualización y delimitación de funciones

· Concentración de responsabilidades
· Las áreas en que están instaladas las tecnologías no cuentan con las condiciones requeridas (climatización, constructivas, aterramiento, etc.)
· Utilización de TIC para el procesamiento y/o transmisión de información no adecuada o autorizada.
· Utilización de TIC para el procesamiento de información sin adoptar las medidas requeridas
· No utilización o utilización incorrecta del cifrado en los casos en que se requiere
· No utilización o utilización inadecuada de la autenticación
· Passwords triviales
· Indisciplina en cuanto al cumplimiento de normas y procedimientos establecidos.

Anexo 9

Instrumento para determinar la competencia de los expertos.

Estimado (a) colega: _____

Teniendo en cuenta su experiencia y cualidades profesionales así como sus características personales, le invito a participar como especialista de un grupo el cual se encargará de hacer valoraciones críticas de una guía metodológica para evaluar el control interno de las Tecnologías Informáticas.
Resulta de gran interés para la autora los criterios y opiniones que usted pueda emitir.
Si esta de acuerdo con nuestra invitación solicitamos de usted que complete el siguiente cuestionario.

¡Muchas Gracias!

Titulo obtenidos: _____

Centro de trabajo: _____

Años de experiencia: _____.

Labor que realiza: _____

1. Realice una autovaloración sobre los conocimientos que usted posee sobre la temática antes expuesta. (coeficiente de conocimiento Kc.)

Experto No.	0	1	2	3	4	5	6	7	8	9	10
1											
2											
3											
n											

(Ningún conocimiento valor 0, hasta el máximo de conocimiento e información valor10)

2. Marque con una x las fuentes que han influido más en el nivel de conocimiento que tiene de la temática en cuestión.(coeficiente de argumentación)

Tabla con las fuentes de argumentación:

Fuentes de argumentación	**Grado de influencia de cada una de las fuentes según sus criterios.**		
	A	**M**	**B**
	(Alto)	**(Medio)**	**(Bajo)**
Análisis teóricos realizados por Ud.			
Experiencia obtenida en su trabajo			
Trabajo de autores nacionales			
Trabajo de autores extranjeros			
Su intuición			

Anexo No. 10

Relación de los expertos que participaron en la aplicación del método Delphi.

No	Centro de laboral	Nivel académico/ Cat. Científica	Años de Experiencia
1	Especialista Gral OSRI[36]	Ing.	17
2	Contralora Provincial – CGR.	MsC	12
3	Directora Provincial JCCE[37]	MsC	16
4	Auditor Jefe Grupo CGR	Lic.	30
5	Unidad Gestión CITMA	Dr.	32
6	Auditor Adjunto CGR – Esp. Informático	Ing	14
7	Grupo de Experto MINED	Lic	16

[36] OSRI – Oficina de Seguridad para las Redes Informáticas -Cienfuegos
[37] JCCE – Joven Club de Computación y Electrónica

	Coeficiente de Conocimientos											Coeficiente de argumentación																			
												Análisis Teórico			Experiencia Obtenida			Trabajo con A nacionales			Trabajo con autores extranjeros			Propio conocimiento del problema			Su intuición				
E	1	2	3	4	5	6	7	8	9	10	Total	A	M	B	A	M	B	A	M	B	A	M	B	A	M	B	A	M	B	Ka	K
												0.3	0.2	0.1	0.5	0.4	0.2	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05	0.05		
1									9		0.9	0.3			0.5					0.05			0.05		0.05					0.05	1.05	0.98
2							7				0.7	0.3			0.5			0.05				0.05			0.05			0.05			1.0	0.85
3						6					0.6		0.2			0.4			0.05				0.05			0.05					0.8	0.70
4								8			0.8		0.2		0.5			0.05				0.05		0.05						0.05	0.95	0.88
5							7				0.7		0.2			0.4		0.05					0.05			0.05		0.05			0.8	0.75
6									9		0.9	0.3			0.5					0.05		0.05			0.05						1.0	0.95
7								8			0.8		0.2			0.4			0.05			0.05			0.05					0.05	0.85	0.83

Leyenda: **Ka: Coeficiente de argumentación.**
Kc: Coeficiente de conocimientos.
K: Coeficiente de competencia.

Fórmula para determinar el índice de competencia K

$K = \frac{1}{2}(K_c + K_a)$ Debe cumplirse que 0,25 ≤ K ≤ 1,0. Para 0,5 ≤ K < 0,8 se considera que el grado de conocimientos es medio y para 0,8 ≤ K ≤ 1,0 se considera alto.

Anexo 11

ENCUESTA PARA RECOGER LAS OPINIONES DE LOS ESPECIALISTAS SOBRE LA CALIDAD Y PERTINENCIA DE LA GUIA ELABORADA

Estimado (a) colega:_____

Después de haber conocido su disposición para participar como parte del grupo de especialista que tendrá a su cargo la valoración de la pertinencia y posible efectividad de la Guía metodológica para evaluar la efectividad del Sistema de Control interno de la actividad informática. Le hacemos llegar la guía y el cuestionario que deberá completar sobre la base de sus criterios al respecto.
Para completar el cuestionario le pedimos que lea usted atentamente las sugerencias que le brindamos a continuación:

1. Realice una valoración crítica de la Guía.
2. Realice una lectura minuciosa de cada de uno de los indicadores que deberá tener en cuenta para emitir sus criterios.
3. Una vez que haya elaborado una valoración definitiva, otorgue la puntuación que corresponda: (5) Muy adecuado, (4) Bastante adecuado, (3) Adecuado, (2) Poco adecuado y (1) No adecuado.
4. Le pedimos además que agregue cualquier opinión personal y sugerencia que usted estime pertinente, independientemente de que ello esté planteado o no de forma explícita.

¡Muchas Gracias!

CUESTIONARIO

1. Exprese sus criterios valorativos en cada uno de los indicadores que aparecen a continuación

I.- Calidad de la propuesta (Guía metodológica)

INDICADORES	**CATEGORÍAS**				
	1	2	3	4	5
I. Estructura de la información					
II. Calidad de la información					
III. Precisión y balance de los aspectos relacionados					
IV. Relevancia y relación con la legislación vigente					
V. Facilidad de empleo como herramienta de consulta					

Señalamientos:_____
_____
_____
_____
_____

Sugerencias:_____
_____
_____
_____

II. – Posibilidades de implementación en la práctica

INDICADORES	CATEGORÍAS				
	1	2	3	4	5
I. Posibilidades de la guía metodológica para mejorar la calidad y desarrollo de las acciones de control relacionadas con el control de las TICs.					
II. Posibilidades de la guía para mejorar la cultura informática de los auditores del sistema.					
III. – Valor científico y metodológico de la guía elaborada.					
IV. Posibilidades de generalización de la guía.					

Señalamientos:_____
_____
_____
_____
_____

Sugerencias:_____
_____
_____
_____