

AUDITORÍA DE LA TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE CAC'S

I. INTRODUCCIÓN	3
II. OBJETIVO	5
III. CONCEPTOS GENERALES	6
A. AUDITORIA DE SISTEMAS.....	6
B. ADMINISTRACIÓN INFORMÁTICA.....	6
C. CONTROL INTERNO.....	6
D. RIESGO.....	7
E. RIESGOS DE NEGOCIO RELACIONADOS CON LA INFORMÁTICA.....	7
1. <i>Riesgos de Integridad</i>	7
2. <i>Riesgos de relación</i>	8
3. <i>Riesgos de acceso</i>	9
4. <i>Riesgos de utilidad</i>	9
5. <i>Riesgos en la infraestructura</i>	10
6. <i>Riesgos de seguridad general</i>	11
F. LA SEGURIDAD INFORMÁTICA Y SUS OBJETIVOS	11
1. <i>Estrategias y políticas</i>	12
2. <i>Administración de la organización</i>	12
3. <i>Monitorización de eventos</i>	13
4. <i>Tecnología informática</i>	13
IV. EL PROCESO DE LA AUDITORIA DE TECNOLOGÍA DE INFORMACIÓN	15
A. PLANEACIÓN DE LA AUDITORIA	15
1. <i>Conocimiento general de la CAC</i>	15
2. <i>Conocimiento del área de Informática</i>	16
3. <i>Memorando de Planeación</i>	16
B. EJECUCIÓN	17
1. <i>Evaluación del Sistema de Control Interno (COBIT)</i>	17
2. <i>Evaluación de las políticas de seguridad informática (ISO 17799)</i>	20
C. INFORME	21
V. TÉCNICAS DE AUDITORIA DE TECNOLOGÍA DE INFORMACIÓN	23
A. PRUEBAS DE CUMPLIMIENTO.....	23
B. PRUEBAS SUSTANTIVAS	23
C. TÉCNICAS DE AUDITORIA ASISTIDAS POR COMPUTADOR.....	24
1. <i>Para probar controles en aplicaciones</i>	24
2. <i>Para auditar centros de procesamiento de información</i>	25
VI. INDICADORES DE GESTIÓN	25

VII. ANEXOS	27
No. 1. AUDITORIA A LAS APLICACIONES	27
No. 2. AUDITORIA AL CENTRO DE COMPUTO.....	30
No. 3. AUDITORIA A NUEVOS DESARROLLOS.....	34
No. 4. TÉCNICAS PARA AUDITAR BASES DE DATOS.....	35
No. 5. POLÍTICAS PARA LA ADMINISTRACIÓN DE LOS RECURSOS TECNOLÓGICOS DE UNA CAC.....	41
No. 6. AUDITORIA A LOS MICROCOMPUTADORES Y REDES LAN	45

I. INTRODUCCIÓN

Para mantenerse competitivos y prestar cada vez mejores servicios a sus asociados, las Cooperativas de ahorro y crédito (CAC's) destinan gran parte de sus recursos financieros al fortalecimiento de sus sistemas de información. Por lo anterior, las directivas como las mismas áreas de tecnología de las CAC's, requieren de herramientas que les permitan evaluar su gestión frente a la adecuada planeación, uso y aprovechamiento que están dando a los recursos de tecnología informática, como determinar si las áreas de tecnología están cumpliendo con su misión y contribuyendo a los objetivos de la CAC.

A&C Consultoría y Auditoría Empresarial (entidad cooperativa colombiana) preparó este documento, con el propósito de proporcionar a la Gerencia, a la Auditoría (interna o externa) como a los directores de tecnología de la CAC's, una guía de evaluación de su gestión sobre los recursos de tecnología, con el ánimo de propender por un mejor control sobre la administración de los recursos tecnológicos de sus entidades, basados en las técnicas de la Auditoría de Sistemas.

Este documento se apoya en el modelo internacional COBIT (Objetivos de Control para la Información y Tecnologías afines, preparado por la Asociación de Auditoría y Control en Sistemas de Información ISACA) y en la norma ISO/IEC 17799, (Código de buenas prácticas de la Gestión de la Seguridad de la Información, desarrollado por la Organización Internacional de Normalización ISO y la Comisión Electrónica Internacional IEC), los cuales son complementarios y no excluyentes.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para mejorar las prácticas de control y seguridad de las Tecnologías de Información (TI), proveyendo un marco de referencia para la Administración, Usuarios y Auditores. Se fundamenta en la identificación de procesos de tecnología de información y sus objetivos de control relacionados. COBIT está orientado a ser la herramienta de administración de tecnologías de información que ayude al entendimiento y a la administración de riesgos asociados con tecnología de información y con tecnologías relacionadas.

La norma ISO/IEC 17799 en una normativa de carácter internacional, considerada como una buena guía para las empresas que pretenden mantener de forma segura sus activos, se fundamenta en 10 áreas de control que serán abordadas a lo largo de este documento.

Nota de los autores¹: con este documento no se pretende agotar el tema de COBIT y la ISO/IEC 17799, solo sirvieron de apoyo para resaltar algunos aspectos que de acuerdo con nuestra experiencia, se consideran vitales para las CAC's, en la administración y control de la TI.

¹ Barón M., César Antonio, socio auditor de sistemas de A&C, y Ramírez B., Luis Humberto, socio gerente general de A&C. Colombia.

II. OBJETIVO

El presente documento tiene como objetivo proveer una guía rápida y concisa para evaluar los procesos relacionados con la automatización de las CAC's.

Ilustra sobre los aspectos que contempla el trabajo de la Auditoría de sistemas, como son: (i) la Planeación de la Auditoría, (ii) la Ejecución, donde se determina la forma de evaluar los procesos relacionados con la sistematización de las CAC's mediante la identificación de los controles y riesgos asociados y (iii) las técnicas de auditoría de sistemas llamadas CAAT's.

Puesto que el tamaño y complejidad de la tecnología utilizada por las CAC's puede ser variada, este documento está desarrollado de manera general, por lo tanto, puede que algunos aspectos no apliquen al momento de realizar su evaluación, u otros aspectos requieran de apoyo en la documentación sugerida al final del documento.

Como apoyo adicional, al final del presente documento se anexan algunos cuestionarios y listas de chequeo, que pueden aplicarse de manera general a cualquier CAC, esperando que sirvan de apoyo en el propósito de evaluar si se administra y controla adecuadamente la tecnología informática de las entidades.

III. CONCEPTOS GENERALES

Para una mejor comprensión del tema, se incluirán algunos conceptos básicos necesarios para realizar una adecuada evaluación de los riesgos y controles de la tecnología informática:

A. AUDITORIA DE SISTEMAS

Es el examen objetivo, crítico, sistemático, posterior y selectivo que se hace a la administración informática de una organización, con el fin de emitir una opinión acerca de:

- la eficiencia en la adquisición y utilización de los recursos informáticos,
- la confiabilidad, la integridad, la seguridad y oportunidad de la información,
y
- la efectividad de los controles en los sistemas de información.

El alcance de la auditoría estará determinado de acuerdo con el objeto a auditar, el cual está compuesto básicamente por todos los recursos informáticos (personas, equipos, aplicaciones, capacitación, etc.), la información y los controles.

B. ADMINISTRACIÓN INFORMÁTICA

Comprende la aplicación del proceso administrativo, en términos de planeación, organización, dirección y control, expresados en hardware, software, datos, factor humano y otros recursos asociados a la automatización las actividades operativas de las organizaciones.

C. CONTROL INTERNO

El sistema de control interno² es un proceso realizado por el consejo de administración (junta directiva o junta de directores), los administradores y demás personal de una entidad, diseñado para proporcionar seguridad razonable en la búsqueda del cumplimiento de los siguientes objetivos:

-Efectividad y Eficiencia de las Operaciones: es decir, en cuanto al cumplimiento de los objetivos estratégicos de la organización (sean estos

² Definición contenida en el documento Internal Control – Integrated Framework, issued by the Committee of Sponsoring Organizations of the Treadway Comisión. Traducida al español por Samuel Alberto Mantilla y editada por Ecoe Ediciones. Segunda edición, marzo de 2000.

comerciales, sociales, de rentabilidad y financieros) y la salvaguarda o protección de sus recursos y los bienes de terceros que se encuentran en su poder de la entidad,

-Suficiencia y Confiabilidad de la Información financiera y la que se produce para uso interno, así como de la preparación de los estados financieros con destino a terceros, y

-Cumplimiento de la Regulación: en general las disposiciones que afectan el desarrollo institucional, tales como las leyes, normas del gobierno, los estatutos, los reglamentos, las circulares o instrucciones internas.

En otras palabras un sistema de control interno efectivo proporciona razonable seguridad de alcanzar esos tres (3) grandes objetivos. Ya con anterioridad se explicó por qué no brinda seguridad absoluta.

D. RIESGO

Es la incertidumbre de que ocurra un acontecimiento que pudiera afectar el logro de los objetivos. También se define como la posibilidad de que suceda algo que tendrá impacto en los objetivos. Se mide en términos de consecuencia y posibilidad de ocurrencia.

E. RIESGOS DE NEGOCIO RELACIONADOS CON LA INFORMÁTICA

Los principales riesgos informáticos de los negocios son los siguientes:

1. Riesgos de Integridad

Abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:

- *Interfaz del usuario*: Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de funciones. Otros riesgos en esta área se relacionan con

controles que aseguren la validez y completitud de la información introducida dentro de un sistema.

- *Procesamiento*: Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles de detección (que son ex post) y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.
- *Procesamiento de errores*: Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de errores (*exceptions*) sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.
- *Interfaz*: Los riesgos en esta área generalmente se relacionan con controles preventivos y de detección que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.
- *Administración de cambios*: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuada de procesos de cambios organizacionales que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.
- *Información*: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos. La integridad puede perderse por: errores de programación (*buena información es procesada por programas mal contruidos*), procesamiento de errores (*transacciones incorrectamente procesadas*) o administración y procesamiento de errores (*administración pobre del mantenimiento de sistemas*).

2. Riesgos de relación

Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la

información de toma de decisiones (*información y datos correctos de una persona /proceso/ sistema en el tiempo preciso permiten tomar decisiones correctas*).

3. Riesgos de acceso

Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: los de segregación inapropiada de trabajo, los asociados con la integridad de la información de sistemas de bases de datos y los asociados con la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:

- *Procesos de negocio:* Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.
- *Aplicación:* La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.
- *Administración de la información:* El mecanismo provee a los usuarios acceso a la información específica del entorno.
- *Entorno de procesamiento:* Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.
- *Redes:* En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.
- *Nivel físico:* Protección física de dispositivos y un apropiado acceso a ellos.

4. Riesgos de utilidad

Estos riesgos se enfocan en tres diferentes niveles de riesgo:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación / restauración usadas para minimizar la ruptura de los sistemas.

- Backups y planes de contingencia controlan desastres en el procesamiento de la información.

5. Riesgos en la infraestructura

Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (*hardware, software, redes, personas y procesos*) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (*servicio al cliente, pago de cuentas, etc.*). Estos riesgos se consideran en el contexto de los siguientes procesos informáticos:

- ☞ *Planeación organizacional:* Los procesos en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio. Además, verifica si existe una adecuada organización (*gente y procesos*), asegura que los esfuerzos de la tecnología informática sea exitosa.
- ☞ *Definición de las aplicaciones:* Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio. Estos procesos abarcan: la determinación de comprar una aplicación ya existente o desarrollar soluciones a la medida. Estos procesos también aseguran que cualquier cambio a las aplicaciones (*compradas o desarrolladas*) sigue un proceso definido que confirma que los puntos críticos de proceso/control son consistentes (*todos los cambios son examinados por usuarios antes de la implementación*).
- ☞ *Administración de seguridad:* Los procesos en esta área aseguran que la organización está adecuadamente orientada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.
- ☞ *Operaciones de red y computacionales:* Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado. También aseguran

que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.

- ☞ *Administración de sistemas de bases de datos:* Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de definición, correspondan con los requerimientos y reduzcan el potencial de redundancia.
- ☞ *Información / Negocio:* Los procesos en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan.

6. Riesgos de seguridad general

Se pueden catalogar como aquellos a los que está expuesto cualquier de los elementos de tecnología, que se minimizan cumpliendo con los estándares proporcionados por la IEC/950 sobre los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:

- ☞ *Riesgos de choque de eléctrico:* niveles altos de voltaje.
- ☞ *Riesgos de incendio:* inflamabilidad de materiales.
- ☞ *Riesgos de niveles inadecuados de energía eléctrica.*
- ☞ *Riesgos de radiaciones:* ondas de ruido, de láser y ultrasónicas.
- ☞ *Riesgos mecánicos:* inestabilidad de las piezas eléctricas.

F. LA SEGURIDAD INFORMÁTICA Y SUS OBJETIVOS

La amplia utilización de los sistemas informáticos en las organizaciones, ha incrementado la necesidad de adoptar toda serie de herramientas y procedimientos para proteger sus sistemas de información, lo que ha puesto en vigencia la importancia de la seguridad informática. El objetivo principal de la seguridad informática es proteger los recursos informáticos del daño, la alteración, el robo y la pérdida. Esto incluye los equipos, los medios de almacenamiento, el software, los listados de impresora y en general, los datos.

Una efectiva estructura de seguridad informática se basa en cuatro técnicas de administración de riesgos, mostradas en el siguiente diagrama:

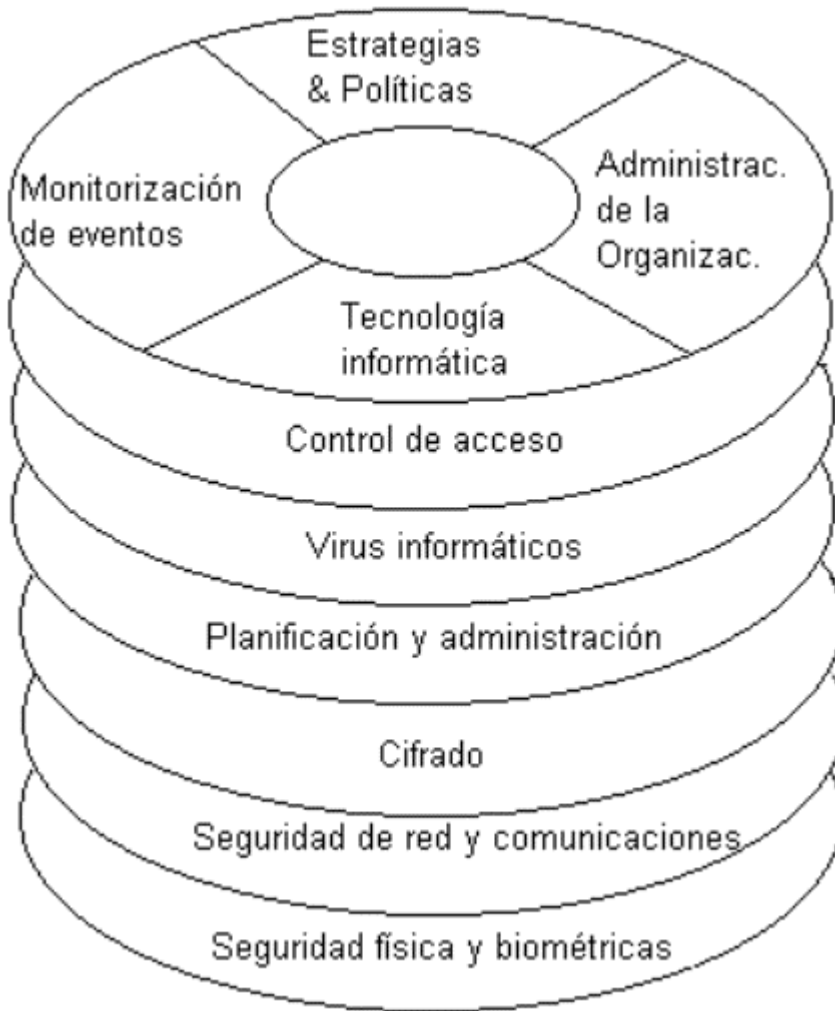


Figura No. 1 Estructura de la seguridad informática

1. Estrategias y políticas

Estrategias de administración para seguridad informática y políticas, estándares, guías o directivas usadas para comunicar estas estrategias a la organización.

2. Administración de la organización

Procesos que se dirigen hacia políticas profesionales y programas de capacitación, administración de cambios y control, administración de seguridad y otras actividades necesarias.

3. Monitorización de eventos

Procesos reactivos que permite a la administración medir correctamente la implementación de políticas e identificar en qué momento las políticas necesitan cambios.

4. Tecnología informática

Es la tecnología necesaria para proveer la apropiada protección y soporte en los distintos procesos involucrados en la organización. La seguridad informática abarca un amplio rango de estrategias y soluciones, tales como:

☞ *Control de acceso:* Una de las líneas de defensa más importantes contra los intrusos indeseados es el control de acceso. Básicamente, el papel del control de acceso es identificar la persona que desea acceder al sistema y a sus datos, y verificar la identidad de dicha persona. La manera habitual de controlar el acceso a un sistema es restringir la entrada a cualquiera que no tenga un nombre de usuario y una contraseña válidos. Las contraseñas son un ejemplo de una forma simple pero efectiva de control de acceso.

El control de acceso es efectivo para mantener a las personas desautorizadas fuera del sistema. Sin embargo, una vez que alguien está dentro, la persona no debería tener acceso libre a todos los programas, archivos e información existente en el sistema. El control de acceso discrecional, se realiza en muchos sistemas, y es una parte importante de cualquier acceso donde el acceso a los archivos y programas se concede en función de la clase de permisos otorgados a un usuario o un perfil de usuarios. Es discrecional en tanto que un administrador puede especificar la clase de acceso que decide dar a otros usuarios del sistema.

☞ *Virus informáticos:* La prevención y control de los efectos producidos por las diferentes clases de virus y programas destructivos que existen.

☞ *Planificación y administración del sistema:* Planificación, organización y administración de los servicios relacionados con la informática, así como políticas y procedimientos para garantizar la seguridad de los recursos de la organización.

☞ *Cifrado:* La encriptación y la desencriptación de la información manipulada, de forma que sólo las personas autorizadas pueden acceder a ella.

- ☞ *Seguridad de la red y de comunicaciones:* Controlar problemas de seguridad a través de las redes y los sistemas de telecomunicaciones.

- ☞ *Seguridad física:* Otro aspecto importante de la seguridad informática es la seguridad física de sus servicios, equipos informáticos y medios de datos reales; para evitar problemas que pueden tener como resultado: Pérdida de la productividad, pérdida de ventaja competitiva y sabotajes intencionados. Algunos de los métodos para prevenir el acceso ilegal a los servicios informáticos incluyen:
 - ☑ Claves y contraseñas para permitir el acceso a los equipos.
 - ☑ Uso de cerrojos y llaves.
 - ☑ Fichas o tarjetas inteligentes.
 - ☑ Dispositivos biométricos (identificación de huellas dactilares, lectores de huellas de manos, patrones de voz, firma/escritura digital, análisis de pulsaciones y escáner de retina, entre otros).

IV. EL PROCESO DE LA AUDITORIA DE TECNOLOGÍA DE INFORMACIÓN

La realización de la evaluación planteada en este documento, contempla las mismas fases que sigue una auditoría de sistemas o de tecnología de información, a saber: (i) planeación, (ii) ejecución e (iii) informe. Se plantea de esta forma para que los administradores y auditores de la tecnología, de manera objetiva, apoyados en esta herramienta, evalúen la gestión en la administración de los recursos tecnológicos de las CAC's.

A. PLANEACIÓN DE LA AUDITORIA

La auditoría de sistemas requiere de una adecuada planeación, con el fin de **definir claramente** los objetivos y el alcance del trabajo, las técnicas y herramientas a utilizar, los recursos humanos, financieros y técnicos que se emplearán, así como los plazos para realizar la evaluación (cronograma).

El objetivo de la planeación es el de proveer al auditor de un conocimiento general de los procesos sistematizados de la organización, una evaluación preliminar de las fortalezas y debilidades y una lista de materias relacionadas con el área que sean de potencial importancia para ser examinadas en la fase de ejecución.

La fase de planeación básicamente comprende:

- Conocimiento general de la CAC
- Conocimiento del área de informática
- Programa de trabajo

1. Conocimiento general de la CAC

Esta etapa permite conocer y estudiar en forma general la entidad y el desarrollo tecnológico en el área de informática, para lo cual es necesario obtener información relacionada con la organización que a criterio del auditor sea suficiente para conocer sus objetivos, reglamentos, normas, funciones, los sistemas de información automatizados, la arquitectura de red, las aplicaciones existentes, etc.

La evaluación de este punto, como parte de la administración de la CAC, permite concluir si se cuenta con documentación actualizada que de manera rápida y precisa permita presentar la entidad a personas que se vinculen y a entidades que deseen conocerla, ya sea para establecer relaciones

comerciales o para ejercer vigilancia y control en el caso de las Superintendencias y los mismos auditores. ¿Qué tanto conocemos nuestra entidad?

2. Conocimiento del área de Informática

Este conocimiento se enfoca a determinar qué tan adecuadamente se tiene documentada la información del área Informática como del sistema de información, verificando si tienen identificadas las debilidades y fortalezas, como todas las relaciones del área con el entorno.

Para planear la evaluación de manera efectiva, se debe determinar la documentación con que se cuenta, calificando su actualización y vigencia, sobre los siguientes aspectos:

- Organización: organigrama donde se ubique el área de tecnología dentro de la organización y el detalle de su estructura, con número de personas por unidad y, en lo posible, los nombres de los colaboradores que pertenecen a cada una de ellas, su perfil técnico, funciones, persona a cargo (si las tiene) y responsabilidades.
- Procedimientos técnicos y administrativos.
- Políticas de seguridad, compras, administración de recursos, capacitación y contratación.
- Distribución física de los equipos, sistemas de seguridad y áreas usuarias.
- Inventario informático, costos de los recursos informáticos y demás información que se considere relevante para el área.

Se espera que terminada la evaluación, la información que detalla cada uno de los aspectos que involucran la tecnología informática de la CAC, estará actualizada y totalmente documentada. El grado de documentación dependerá de la complejidad y alcance que se defina tener en cada CAC.

3. Memorando de Planeación

Los programas que se expresan como planes de trabajo y conforman el memorando de planeación, contienen, cuando menos, lo siguiente:

- la definición de las actividades o aspectos a cubrir en la fase de ejecución, las cuales se determinan de acuerdo con las debilidades que se identifican durante de las dos etapas anteriores, priorizando aquellos aspectos que se observen de mayor riesgo, de bajo control y que estén soportando los procesos críticos de la CAC. No obstante y con el apoyo de las listas de chequeo generales (que se incluyen en de este documento), se podrían identificar aspectos que a primera vista se

consideren adecuadamente administrados y controlados, pudieran no estarlo tanto y hacer que se reenfoque el trabajo planeado y su alcance.

- la disposición de tiempo, modo y lugar de los recursos necesarios y
- su justificación para llevar a cabo la auditoría.

B. EJECUCIÓN

Esta fase consiste en ejecutar los programas de trabajo establecidos en el memorando de planeación, mediante:

- la evaluación del sistema de control interno del área de informática (incluye la seguridad informática),
- la evaluación de la gestión de la entidad en la administración de los recursos de tecnológicos de información, y
- la realización de pruebas para tener un concepto objetivo del estado actual del sistema de control interno de la CAC.

1. Evaluación del Sistema de Control Interno (COBIT)

Se debe identificar y evaluar que los controles implementados permitan prevenir y detectar oportunamente los acontecimientos que impidan el cabal cumplimiento de las políticas, procedimientos, planes, y objetivos de la entidad y que tengan directa relación con la información tecnológica y de sistemas.

Se debe evaluar si el control cumple con los principios de:

- **Efectividad:** Se refiere a que la información relevante sea pertinente para el proceso de la CAC, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- **Eficiencia:** Se refiere a la provisión de información a través del óptimo (más productivo y económico) uso de los recursos.
- **Confidencialidad:** Relativa a la protección de la información sensitiva de su revelación no autorizada.
- **Integridad:** Se refiere a la exactitud y suficiencia de la información, así como su validez, en concordancia con los valores y expectativas de la entidad.
- **Disponibilidad:** Se refiere a que la información debe estar disponible cuando sea requerida por los procesos de la entidad ahora y en el

futuro. Involucra la salvaguarda de los recursos y sus capacidades asociadas.

- **Cumplimiento:** Se refiere a cumplir con las leyes, regulaciones y acuerdos contractuales, a los que están sujetos los procesos de la entidad.
- **Confiabilidad:** Se refiere a la provisión de la información apropiada a la alta gerencia, para operar la entidad, tomar decisiones y evaluar la gestión realizada.
- **Planeación:** Que las decisiones tomadas sobre la adquisición e implantación de recursos informáticos obedezca a las políticas de la entidad y se encuentren enmarcados dentro de un plan estratégico.

Los recursos que deben ser evaluados en el cumplimiento de los anteriores principios se han identificado como:

- **Datos:** Los elementos de datos internos, externos, estructurados, no estructurados, gráficos, sonidos, etc.
- **Aplicaciones:** Es la suma de procedimientos manuales y programados.
- **Tecnología:** Cubre hardware, software, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.
- **Instalaciones:** Recursos para alojar y dar soporte a los sistemas de información.
- **Personal:** Habilidades del personal, conocimientos, conciencia y productividad para planear, organizar, adquirir, entregar, soportar, y monitorear servicios y sistemas de información.

Una vez finalizada la fase de evaluación del Sistema de Control Interno, se revisa el memorando de planeación, de manera que puedan incluirse ajustes a las siguientes fases de la ejecución de la auditoría, de ser necesario para incluir otras áreas críticas identificadas.

Las áreas de influencia (dominios) a tener en cuenta en el proceso de evaluación son:

- **Planeación y Organización:** Se deben evaluar los controles existentes para la ejecución del plan estratégico, la arquitectura de la información, administración de los sistemas de información, dirección y

administración del área de sistemas, administración de proyectos, administración del recurso humano.

- **Adquisición e implementación:** Se refiere a aquellos procedimientos implementados por la entidad para hacer más efectiva, eficiente y económica la adquisición de recursos tecnológicos de sistemas.

Se deben identificar los controles existentes para los contratos de adquisición de software (aplicaciones, licencias, sistemas operativos, correo electrónico, Internet, etc.), y hardware (equipos, redes, etc).

- **Entrega de servicios y soporte:** Se evalúan los controles que tiene la entidad para garantizar que se cumpla con el objeto de los contratos de outsourcing (tercerización) y servicios prestados.

Se evalúan los programas de capacitación de los usuarios, la atención a los usuarios, la administración de la configuración, de los datos, de las instalaciones, operaciones.

- **Monitoreo:** Se refiere a la evaluación de los procedimientos implementados para hacer un seguimiento y una auditoría interna de todos los procesos relacionados con la informática, bien sea día a día o en forma periódica para verificar su efectividad. Igualmente a los procedimientos que se han incorporado a los sistemas de información tecnológica para hacer un seguimiento de las actividades realizadas por los usuarios.

Los controles pueden estar incluidos, de un modo intrínseco, en las actividades recurrentes de una entidad o consistir en una evaluación periódica independiente, llevada a cabo normalmente por la dirección. La frecuencia de estas evaluaciones depende del juicio de la dirección. Mediante estos controles podremos detectar errores significativos y realizar un control continuo de la fiabilidad y de la eficacia de los procesos informáticos.

- **Documentación:** La Entidad debe tener políticas claras y por escrito sobre la documentación del área de sistemas y el plan estratégico de sistemas de información. Los sistemas de aplicación, los programas del sistema operativo, los equipos de cómputo, las redes de datos, los periféricos, las funciones y responsabilidades, la operación del centro de cómputo, las decisiones de cambios de equipos y aplicaciones, los estándares para el diseño y desarrollo, entre otras, deben estar suficientemente documentadas para la comprensión completa y exacta

de las actividades de sistemas de información automatizados y su impacto en los usuarios.

2. Evaluación de las políticas de seguridad informática (ISO 17799)

Como complemento de la evaluación del control interno y como un punto de referencia, se debe tener en cuenta durante la evaluación a realizar, las diez áreas de control propuestas por la norma internacional ISO 17799, a efecto de diagnosticar el sistema de seguridad frente a los estándares aceptados internacionalmente, si en algún momento se quisiera certificar el aspecto de seguridad en la CAC.

- **Política de seguridad:** Se necesita una política que refleje las expectativas de la organización en materia de seguridad con el fin de suministrar administración con dirección y soporte, la cual también se puede utilizar como base para el estudio y evaluación en curso.
- **Organización de la seguridad:** Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.
- **Control y clasificación de los recursos de información:** Necesita un inventario de los recursos de información de la organización y con base en este conocimiento, asegurar que se brinde un nivel adecuado de protección.
- **Seguridad del personal:** Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la CAC. Se debe implementar un plan para reportar los incidentes.
- **Seguridad física y ambiental:** Responde a la necesidad de proteger las áreas, el equipo y los controles generales.
- **Manejo de las comunicaciones y las operaciones:** Los objetivos de esta sección son:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
 - Minimizar el riesgo de falla de los sistemas.
 - Proteger la integridad del software y la información.
 - Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
 - Garantizar la protección de la información en las redes y de la infraestructura de soporte.
 - Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
 - Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.
-
- **Control de acceso:** Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

 - **Desarrollo y mantenimiento de los sistemas:** Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

 - **Manejo de la continuidad de la empresa:** Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes, en caso de una falla grave o desastre.

 - **Cumplimiento:** Imparte instrucciones para que se verifique si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

C. INFORME

Resultado de la evaluación, se debe preparar un informe el cual, además de ser claro, preciso, conciso, veraz, objetivo y de presentar hechos reales debidamente sustentados, debe dar las pautas para un plan de mejoramiento de los controles y seguridades establecidas dentro del sistema de información. Sirve además para fortalecer la administración de la tecnología informática de las CAC, se constituyen en otra herramienta para soportar las inversiones necesarias en

tecnología ante la alta gerencia y afrontar de manera satisfactoria las auditorías que se realicen al área de tecnología de nuestras CAC.

V. TÉCNICAS DE AUDITORIA DE TECNOLOGÍA DE INFORMACIÓN

Los procedimientos en auditoría requieren de técnicas que ayuden a establecer la eficiencia en la adquisición y utilización de los recursos informáticos, la consistencia, integridad y oportunidad de la información y la efectividad de los controles.

Las pruebas de auditoría constituyen la base con que el auditor obtiene evidencias adecuadas que le permiten estructurar los hallazgos, los cuales fundamentan las conclusiones de la ejecución de la auditoría. Los hallazgos, sin descartar otros aspectos, son las debilidades (u oportunidades de mejoramiento) que se deben tomar en cuenta para fortalecer el sistema de control interno.

Las pruebas que se pueden realizar sobre los sistemas son pruebas sustantivas y pruebas de cumplimiento, tal como se define a continuación:

A. PRUEBAS DE CUMPLIMIENTO

Se usan para determinar si un procedimiento de control, previamente establecido, está funcionando efectivamente, y consisten en verificar:

- La aplicación de leyes o reglamentos y de los procedimientos establecidos en los manuales y que éstos se encuentren actualizados.
- El conocimiento por parte del personal, de los manuales y de las políticas del ambiente informático.
- La existencia del plan estratégico de sistemas, informes o memorandos preparados por el Departamento de Informática.
- Si han sido implantadas las recomendaciones emitidas por auditorías anteriores.

B. PRUEBAS SUSTANTIVAS

Se usan para determinar que existe una seguridad razonable sobre la validez de la información producida. El desarrollo de las pruebas es logrado mediante la aplicación de una o varias técnicas de auditoría, ya sea simultánea o sucesivamente, tales como:

- Analizar registros.
- Hacer operaciones.
- Comparar archivos.

- Estratificar archivos.
- Seleccionar una muestra aleatoria.
- Resumir información.
- Generar reportes.
- Construir archivos de prueba.
- Extraer información de un archivo.
- Realizar análisis estadísticos.
- Simular parte del sistema o el sistema completo.

C. TÉCNICAS DE AUDITORIA ASISTIDAS POR COMPUTADOR

Unas de las herramientas más útiles para adelantar pruebas de cumplimiento y sustantivas, son las que se conocen como técnicas de auditoría asistidas por computador (TAAC), las cuales se orientan hacia los datos, las aplicaciones, los equipos y programas, y permiten seleccionar y procesar la información necesaria para fines específicos de la auditoría, facilitando la aplicación de métodos de muestreo estadístico, aumentar el alcance de las pruebas y verificar la integridad de los datos en la población auditada.

Las TAAC sirven para:

- probar controles en aplicaciones,
- seleccionar y monitorear transacciones,
- verificar datos,
- analizar programas de las aplicaciones,
- auditar centros de procesamiento de información, y
- auditar el desarrollo de aplicaciones.

1. Para probar controles en aplicaciones

Utilizadas para evaluar los controles en aplicaciones sistematizadas y para probar el cumplimiento de los controles existentes en las aplicaciones, a saber:

- **Evaluación del caso base:** Elaborar archivo de prueba y verificar la exactitud de los procesos. Se realiza la prueba en todo el ciclo del sistema.
- **Operación paralela:** Busca verificar el buen desempeño de nuevas aplicaciones, identificar resultados no esperados, comparar lo antiguo con lo nuevo operando conjuntamente.

- **Prueba integrada:** Esta técnica implica tener, como mínimo, la misma capacidad tecnológica en la cual está la aplicación en producción. Se deben procesar archivos de prueba en aplicaciones en producción y comparar los resultados reales versus los esperados.
- **Simulación paralela:** Codificar rutinas que simulen la lógica del programa real, se debe considerar el porcentaje de error en los resultados de la simulación. Se emplea generalmente software generalizado de auditoría y programas a la medida.

2. Para auditar centros de procesamiento de información

Se debe hacer un análisis de datos del JOB accounting, verificar si existe un plan de contingencia y si existen las suficientes medidas de seguridad para salvaguardar y proteger los recursos tecnológicos de informática.

Para realizar la evaluación del sistema de información tecnológica se propone hacerlo mediante la utilización de las listas de chequeo anexas al presente documento, las cuales se han desarrollado teniendo en cuenta los tipos de control. Se aclara que estas listas de chequeo son generales, no son excluyentes, ni exhaustivas; por tanto, se deben considerar como una guía en el proceso de evaluación y la profundidad de la evaluación dependerá de la complejidad de la tecnología utilizada por cada CAC, lo que conduciría a depurarlas y actualizarlas, en caso de que se utilicen de manera periódica, de tal forma que nunca pierdan vigencia.

VI. INDICADORES DE GESTIÓN

“Lo que no es medible no es gerenciable, ya que el control se ejerce a través de hechos y datos”

Partiendo de la premisa anterior, es necesario identificar de qué manera se está midiendo la gestión de informática dentro de la CAC. Es por esto que en este punto ponemos a su consideración el uso de esta herramienta de administración, que tiene entre otras las siguientes funciones:

- Permiten la realización de una evaluación del impacto de la gestión realizada. Son utilizados para comparar un plan establecido contra unos valores reales.
- Seguimiento y rendimiento de cuentas.
- Sirven como instrumento de regulación, como base para toma de decisiones, transferencias presupuestales y políticas.

Ejemplos: A continuación se enuncian algunos de los indicadores de gestión que se pueden implementar en el área de tecnología:

NOMBRE	CALCULO	RESULTADO
Eficacia en la gestión	$\frac{\text{No. actividades desarrolladas}}{\text{No. Actividades planeadas (pesi)}}$	Evaluar el cumplimiento del Plan Estratégico de Sistemas (PESI)
Efectividad de documentación Aplicativos	$\frac{\text{No. aplicativos documentados}}{\text{Total aplicativos}}$	Identifica si existe una adecuada documentación
Cubrimiento	$\frac{\text{No. puntos de red}}{\text{No. equipos}}$	Cubrimiento de la red
Eficiencia de los recursos tecnológicos	$\frac{\text{No de computadores en uso}}{\text{Total de computadores}}$	Verifica la productividad de los equipos. Se mide teniendo en cuenta los aplicativos existentes
Eficiencia en la distribución del recurso tecnológico	$\frac{\text{No. Microcomputadores}}{\text{No. funcionarios que necesitan computador}}$	Verifica la adecuada distribución de los recursos
Legalidad	$\frac{\text{No de licencias adquiridas}}{\text{No de aplicativos instalados}}$	Verifica que el software instalado cuente con la licencia
Legalidad	$\frac{\text{No. de licencias por software}}{\text{No equipos en que está instalado}}$	Se puede establecer si el software está debidamente licenciado
Capacitación	$\frac{\text{No. de usuarios capacitados}}{\text{Total de usuarios}}$	Determina la efectividad en la capacitación
Conectividad de recursos compartidos	$\frac{\text{No. Puntos de red}}{\text{No. computadores}} \times 100$	Determina el porcentaje de cubrimiento de las redes de datos

VII. ANEXOS

No. 1. AUDITORIA A LAS APLICACIONES

1. POLÍTICAS Y PROCEDIMIENTOS

- Revisión de los manuales y procedimientos que documentan la aplicación.
- Entrevistas a los usuarios y al personal de sistemas usando los diagramas de flujo de datos para documentar las operaciones que se describan.

2. ESTÁNDARES DE DESARROLLO Y PRODUCCIÓN

- Evaluación del procedimiento de actualización de los estándares.
- Verificar que los mantenimientos efectuados a la aplicación se ajusten a los estándares de desarrollo.
- Revisar el cumplimiento de las políticas de backups.
- Comparación de la descripción de archivos, campos y programas con los que recomienda el estándar.
- Revisar la bitácora de operación, verificando que todos los procesos que se corren queden registrados.
- Verificar que los procesos de almacenamiento y restauración de datos cumplen con los estándares de producción.
- Verificar que la codificación de la aplicación se ajusta al estándar de procedimientos y comandos de producción.

3. DATOS DE ENTRADA

- Revisar los documentos fuente que utilice el paquete verificando su consistencia e integridad en la información. Aspectos a revisar como los siguientes:
 - .1. Legibilidad de la información.
 - .2. Manejo de errores en el documento fuente.
 - .3. Políticas de retención de los documentos.
 - .4. Control de los documentos confidenciales.
 - .5. Almacenamiento de los documentos no diligenciados.
 - .6. Sistema de control sobre documento digitado.
 - .7. Sistema de control de lotes o grupos de documentos procesados.
 - .8. Conservación del consecutivo del documento.
 - .9. Verificar separación de funciones entre quien prepara el documento fuente y quien lo captura en el sistema.

4. PROCEDIMIENTOS DE CAPTURA

- Verificar la validación de los datos que son capturados, mediante pruebas en línea y en ambientes paralelos a los programas respectivos.

- Examinar la metodología de corrección de errores que tienen los programas en su codificación interna.
- Revisar los procedimientos de manejo de errores que son descubiertos durante la captura.

5. PROCEDIMIENTO Y ACTUALIZACIÓN DE INFORMACIÓN

- Ejecución de pruebas a los programas correspondientes a la aplicación.
- Suministro de datos reales y de prueba, verificando a la salida (informes o reportes por pantalla y listados) la consistencia de la información.
- Revisión analítica de los programas fuente para los programas más críticos.
- Verificar la acción de las cifras de control en los programas y procesos que las posean.
- Verificar la consistencia de los campos descritos en los archivos con la información que debe ser almacenada en ellos.
- Observar el método de actualización que evidencian los archivos.
- Analizar los cambios y mantenimientos a los programas verificando las debidas autorizaciones.

6. INFORMES DE COMPUTADOR

- Revisar la estructura de los informes de computador utilizando la matriz de análisis.
- Analizar el origen y destino final de los informes.
- Evaluar el sistema de archivo y retención de los informes de computador.
- Analizar los procedimientos de manejo de error en los listados.
- Verificar el borrado de los archivos magnéticos de impresión luego de ser listados.
- Evaluar la información de salida a la luz del sistema de información requerido por la gerencia.

7. DOCUMENTACIÓN

- Revisar las carpetas fuente de los programas seleccionados a fin de determinar la documentación correspondiente a los estándares de desarrollo.
- Evaluar la existencia de manuales de sistemas, técnicos y de usuario de la aplicación.
- Analizar la documentación que soporta las modificaciones que evidencian los programas.

8. SEGURIDAD

- Evaluar el sistema de seguridad lógico a través del archivo de seguridad y los archivos de usuarios con privilegios.
- Analizar el período de modificación de los password propios de la aplicación.
- Verificación en el log del sistema de los accesos que observan los programas y archivos más críticos.

9. PROCEDIMIENTOS DE RESPALDO

- Evaluar el plan de contingencias de la aplicación y el conocimiento de la misma por parte de los usuarios.
- Evaluar el sistema de backups utilizado para los archivos de datos.

10. CAPACITACIÓN Y SOPORTE A USUARIOS

- Verificar el conocimiento que tienen los usuarios del manejo de los módulos propios de la aplicación.
- Revisar los procedimientos de capacitación que son utilizados para la instrucción de los usuarios.
- Analizar la respuesta que tienen los usuarios a sus problemas tanto de hardware como de programas.

No. 2. AUDITORIA AL CENTRO DE COMPUTO

1. PREGUNTAS CLAVES.

- Procedimientos escritos que se manejan. Manuales por aplicación (sistemas y operación)
- Red instalada en la Empresa.
- Número de servidores.
- Ubicación de los servidores.
- Número de terminales conectadas.
- Número de usuarios conectados al servidor.
- Configuración de memoria y discos de los servidores.
- Protocolos instalados y servicios.
- Volumen de producción mensual de registros de cada aplicación.
- Interfases que manejan.
- Reciben y/o envían archivos a entidades externas.
- Principales proveedores de tecnología.
- Sistemas de seguridad electrónica instalados
- Actualmente se tiene auditoría de sistemas.
- Planes de contingencia para el área de informática.
- Proyectos futuros.

2. CUIDADO DE LAS INSTALACIONES

Ubicación

- Del centro de cómputo.
- Techos, maquinarias especiales.
- Tipo de estantería.
- Ubicación de la luz.

Existe un procedimiento claro de limpieza y aseo para los computadores y el centro de cómputo?

Electricidad

- Hay corriente regulada identificada?
- Tienen reguladores de voltaje?.
- Existen pruebas funcionamiento de la UPS. Las fases deben estar balanceadas?.
- Existe plano eléctrico de la Empresa? (preferiblemente en medio magnético).
- Se hace revisión periódica de los circuitos eléctricos?
- Se cuenta con planta eléctrica?. Se tienen procedimientos claros para su uso y mantenimiento?

Aire Acondicionado

- Hay sistema de aire acondicionado?.
- Verificar si es independiente al de las personas.
- Hay sistema de reserva energética para el aire acondicionado?
- Es suficiente para el área del centro de cómputo? Controla la humedad del aire?

- Se tiene sistema redundante de aire acondicionado?

Protección contra incendios

- Tienen sistema de protección contra incendios?. Revisar si es manual o automático.
- Se hizo capacitación al personal del área para el manejo de los extintores y se ha probado.
- Qué tipo de sustancias tienen los extintores.
- Procedimientos de emergencia.
- Existen normas o actividades ante un desastre?.
- Existen estrategias para la evacuación?.

Seguros

- Revisar el sitio de ubicación del bien.
- Evaluar los procedimientos para el manejo de los seguros.
- Revisar el inventario de equipos de cómputo de la empresa y a la aseguradora.

Hardware

- Tienen seguros todos los computadores?.
- Se aseguran las cintas y otros dispositivos para almacenamiento?.
- Verificar los amparos a los computadores?

Software

- Se aseguran las patentes ó licencias?.
- Hay seguro para horas hombre en recuperación de la información?

Pólizas de manejo.

- Hay pólizas de manejo.
- Cual es su cobertura?
- Quienes están incluidos?

3. OPERACIÓN DE LOS SERVIDORES

Registro o de operaciones.

- Evaluar el manejo de bitácoras manuales en el centro de cómputo.
- Hay registro automático?.
- Cada cuánto se realizan y que acciones se toman?
- Quién las revisa?

Procedimientos del operador.

- Tienen manual de funciones?.
- Sus actividades están basadas en normas claras.
- Hay procedimientos para:
 - Prender el Servidor.
 - Apagar el Servidor.
 - Otorgar permisos en el sistema

Programación de actividades.

- Son programadas las actividades del operador?.

- Manejan cronogramas, planes de trabajo y/o acuerdos de servicio?.

Mantenimiento de archivos maestros.

- Chequeo y/o revisión de las tablas principales del sistema contable y las aplicaciones de misión crítica.
- Evaluar la frecuencia de depuración de los archivos maestros.
- Revisar los procedimientos de depuración de archivos maestros.

4. CONTROL DE ENTRADAS Y SALIDAS.

Entradas

- A qué horas y en que fecha se reciben?
- Qué control hay sobre el documento que se recibe?

Salidas

- Existen hoja de ruta de los informes?
- Se comparan los informes contra los documentos de entrada?

Reconciliación de salidas.

- Con qué frecuencia de realizan contra documentos de terceros?.

5. SEGURIDAD EN INSTALACIONES.

Administración general de la seguridad

- Evaluar los criterios de seguridad que tiene el área de informática.
- Revisar los sistemas de vigilancia.
- Observar las garantías de seguridad del sitio donde está ubicado el centro de cómputo.

Seguridad Externa

- Evaluar los controles de acceso automático.

Seguridad Interna

- Son independientes las áreas de trabajo?.
- Los computadores están ubicados en sitios seguros?.
- Se protegen los equipos con cobertores plásticos?
- Hay canaletas, iluminación y ergonomía en el área?.

6. ORGANIZACIÓN Y PERSONAL

Organización y personal.

- Evaluar criterios de administración.
- Revisar los períodos vacacionales.
- Hay rotación de analistas en su cargo?
- Cuáles son las estrategias de promoción?.
- Revisar los parámetros de ascenso establecidos.

Segregación de funciones.

- Se detecta concentración de funciones en algún empleado?

- Evaluar los criterios del área para difundir o multiplicar conocimientos.
- La capacitación esta relacionada con los proyectos del área?.

7. PLANES DE CONTINGENCIA.

Creación del Plan

- Existen planes de contingencias?.
- Están documentados?.
- Verificar el personal que participa en la definición del plan de contingencias.

Tópicos

Hardware

- Equipo de soporte.
- Acuerdos con otras compañías.
- Acuerdos con los proveedores.
- Dispositivos claves.

Software

- Procedimientos manuales que garanticen la continuidad del servicio.
- Personal
- Existe matriz de sustitutos - Quien reemplaza a quien?
- Difusión del plan.
- Planes de difusión y entrenamiento.
- Pruebas de simulación.

No. 3. AUDITORIA A NUEVOS DESARROLLOS

En Cada punto se enuncia las preguntas a realizar se en cada etapa del desarrollo planeado.

1. PLANEACIÓN Y ANÁLISIS DEL PROYECTO

- Objetivo del proyecto.
- Personal involucrado.
- Cronograma de trabajo.
- Presupuesto.
- Equipos y aplicaciones asociados.
- Participación y aceptación por parte del usuario.
- Aplicación de la metodología de desarrollo.

2. EN LA ETAPA DE DISEÑO

- Revisión del cumplimiento de normas legales, políticas, procedimientos, normas contables y tributarias.
- Períodos de retención de archivos, backup, procedimientos de recuperación.
- Revisión al plan de pruebas y/o conversión de programas.
- Revisión al plan de migración de datos.
- Revisar la matriz de acceso a la aplicación.
- Proponer tablas-auditor para datos críticos, previa discusión con el usuario.
- Sugerir cifras de control para los datos.
- Diseñar y proponer al grupo reportes y consultas de control.

3. CONSTRUCCIÓN Y PRUEBAS

- Revisión a la implantación de controles.
- Revisión a la documentación referida en los estándares.
- Revisión al cumplimiento del presupuesto.
- Revisión a la participación y aprobación del usuario en las pruebas de aplicaciones y pruebas de conversión y/o migración de programas y datos.
- Participación en pruebas a programas.
- Revisión al cumplimiento de los planes de entrenamiento.
- Probar los controles automáticos recomendados.
- Revisión al plan de contingencias de la aplicación.

4. EN CONVERSIÓN E INSTALACIÓN

- Revisión al proceso de conversión.
- Revisión final de los procedimientos.
- Verificar la creación de controles recomendados.
- Verificar la completa aceptación del usuario.
- Verificar la ejecución de pruebas completas antes de instalarse en producción.
- Informar cumplimiento de los presupuestos iniciales.

Nota: Existen otros aspectos que la CAC y la experiencia invitarán a incluir en este documento.

No. 4. TÉCNICAS PARA AUDITAR BASES DE DATOS

A continuación se enuncian algunos criterios para auditar las bases de datos. Para facilitar la comprensión de los aspectos referidos, se toman a manera de ejemplo algunos comandos de seguridad del sistema operacional UNIX y del sistema manejador de bases de datos INFORMIX. Según las herramientas que cada CAC posea, podrá emular los comandos que cumplan similar función.

Para efectuar auditoría a bases de datos, se propone iniciar desde la recopilación de información, y la ejecución de varias pruebas relacionadas con el tratamiento de la información en la base de datos, el uso de comandos críticos tanto en UNIX como en INFORMIX y la utilización de los estándares de desarrollo definidos para cuarta generación.

1. ACTIVIDADES PRELIMINARES

Consiste en la labores de documentación que debe adelantar el auditor luego de planear el programa de auditoría, participar al usuario de la actividades de revisión que se van a efectuar. Las actividades aplican de igual manera tanto para auditar aplicaciones que ya están en funcionamiento como para aquellas en las cuales la participación de auditoría es simultánea al desarrollo de la aplicación. Se recomienda hacer acopio de dicha información mediante el desarrollo de los siguientes pasos:

- Obtener los procedimientos y políticas que soporten las operaciones del área motivo de estudio.
- Identificar para la base de datos, cuáles funcionarios la administran o tienen responsabilidad directa con los datos, quiénes proveen el servicio técnico de mantenimiento o soporte y qué personas son usuarias actuales.
- Obtener los formatos de análisis de seguridad de la aplicación.
- Adquirir la relación del software propio del manejador de la base de datos utilizado en la entidad.
- Recopilar la lista de aplicaciones de la CAC que ingresan o son ingresadas por la base de datos.
- Identificar las interfaz de la aplicación con otros sistemas operacionales diferentes tales como WINDOWS SERVER 2000, UNIX, OS 4000, etc.
- Obtener para la aplicación que se está analizando, la siguiente información:
 - Bases de datos utilizadas
 - Tablas que conforman la base de datos
 - Vistas definidas
 - Índices definidos para las tablas de la base de datos

- Librerías propias del manejador de la base de datos y de la aplicación motivo de estudio.
- Catálogo de sistema manejador o diseñado por los analistas.
- Diccionarios de datos del sistema
- En relación a procedimientos de seguridad, debe adquirirse:
 - Procedimientos de recuperación ante caídas de la aplicación.
 - Acuerdos de soporte en procesamiento con otras empresas.
 - Políticas de contingencias establecidas para las bases de datos.
- Copiar en un ambiente de prueba paralelo un segmento de las bases de datos que van a ser analizadas y los programas seleccionados para la revisión.

2. PRUEBAS A EJECUTAR

Las pruebas a ejecutar se adelantaran de acuerdo a los módulos de procedimientos y políticas, seguridad, desarrollo, participación de usuario, documentación y procedimientos de respaldo y recuperación.

- Procedimientos y políticas: Los procedimientos actuales serán revisados teniendo presente la vigencia, cumplimiento, eficiencia y relación con las demás áreas de la CAC.
- Seguridad
 - Evaluar los derechos de acceso que tienen los usuarios de la aplicación. Para ello debe revisarse en el catálogo de seguridad de Informix los archivos SYSUSERS, SYSTABAUTH Y SYSCOLAUTH.
 - En SYSUSERS se verifica la razonabilidad de los accesos de usuarios a la base de datos.
 - En SYSTABAUTH se analizan los derechos de los usuarios para acceder las diferentes tablas de la base de datos.
 - En SYSCOLAUTH se deben verificar los derechos de los usuarios a determinados atributos de una tabla específica de la base de datos.
 - Para la anterior evaluación deben compararse los formatos de “análisis de seguridad” elaborados durante el diseño de la aplicación con la estructura de derechos que observa la misma en producción. El formato mencionado debe evidenciar la autorización del Jefe de Área usuaria asignada para otorgar los permisos respecto de la aplicación.
 - Tales verificaciones se complementarán con pruebas de línea sobre la base de datos conjuntamente con el usuario responsable.
 - En el Log del sistema, se debe verificar la razonabilidad en la utilización de los comandos GRANT Y REVOKE, por parte de los usuarios y personal de sistemas involucrados con la ejecución de programas y manipulación de las bases de datos. Instrucciones motivo de análisis por parte de auditoría son las afines con GRANT CONNECT TO, GRANT DBA TO, REVOKE ALL FROM, etc. Estas permiten establecer los derechos asignados y retirados durante un período de tiempo.

- Los derechos de ejecución de programas, lectura y escritura de archivos que sean creados desde el sistema operacional UNIX también deben ser evaluados. Debe ser motivo de evaluación periódica el log del sistema para efectuarle seguimiento al uso de los siguientes comandos:
CHMOD: Cambios en la estructura de los permisos ya establecidos.
CHOWN: Cambios de propietarios en las tablas de la base de datos.
CRYPT: Definición de passwords para la ejecución de algunos programas. Debe tenerse presente que el uso de los comandos CHMOD Y CHOWN solo pueden ejecutarse por parte del “superusuario” y por el creador del archivo ejecutable.
- Si las bases de datos creadas tiene LOG TRANSACTION o AUDIT TRAIL, debe revisarse las características de las actualizaciones en la base de datos. Adicionalmente el estado de estos archivos observando el número total de registros y la última fecha de actualización.
- Revisar la revocación del acceso del analista de sistemas si la aplicación ya ha sido entregada a producción.
- Verificar que las bases de datos de prueba están aisladas de las áreas de producción y sean removidas totalmente al momento de terminar la implantación de la aplicación.
- Si el usuario posee control por hora y terminal, evaluar en el log los accesos en atención a la restricción definida.
- Verificar la revocación de todos los permisos a nivel de tabla para los usuarios cuando se hace la asignación de derechos. Probar mediante edición de los catálogos de seguridad.
- Estándares de Desarrollo
 - Evaluar las estrategias de indexación aplicados a las tablas de las bases de datos creadas.
 - Efectuar compilaciones a los programas fuentes para determinar los llamados a SQL incluidos.
 - Revisar el documento de diseño para la aplicación y establecer las tablas propuestas y programas definidos. Posteriormente deben ser listadas las tablas y programas que se encuentran productivos para identificar la coincidencia en ambos documentos.
 - Verificar que los programas, módulos, variables de programa, funciones, reportes, tablas y bases de datos de la aplicación son documentadas de acuerdo a los estándares de desarrollo definidos para cuarta generación.
 - Verificar que las pantallas diseñadas en la aplicación cumplen con los patrones establecidos en los estándares de desarrollo de la empresa.
 - Revisar el diccionario de datos verificando la descripción e integridad de los mismos.
 - Comparar el catálogo SYSTABLES con las tablas seleccionadas para determinar la actualización periódica del mismo.
 - Evaluar el modo de aplicación de la instrucción LOG TABLE cuando se asignen privilegios a nivel de tabla.

- Participación del usuario
 - ☑ Revisar las vistas sugeridas por el usuario, los prototipos definidos y compararlos con las formas y reportes construidos a través de la herramienta SMBD utilizada. En este aspecto la auditoría evaluará mediante la participación activa, la completa satisfacción del usuario frente a la forma como requiere ser presentada su información. Las reuniones y entrevistas con el usuario darán un adecuado apoyo a esta evaluación.
- Documentación
 - ☑ Revisar la bitácora de la base de datos a fin de establecer eventos de interés que incidan en la estructura de la base de datos, tales como inserción de nuevos campos, pérdida de datos o índices, caídas del sistema, etc.
 - ☑ Comparar el software propietario del SMBD descrito en los manuales con una impresión de los archivos que se encuentran en los directorios de producción.
- Respaldo y recuperación
 - ☑ Determinar la frecuencia de respaldos que tiene la base de datos comparando este resultado con la política de backups establecida.
 - ☑ Evaluar los mecanismos de recuperación ante las contingencias que puedan evidenciar la base de datos.

RECOMENDACIONES DE SEGURIDAD ADICIONALES PARA AMBIENTES DE CUARTA GENERACIÓN

Las recomendaciones de seguridad a la información que se relacionan a continuación que describen algunos parámetros a ser tenidos en cuenta cuando son implantados sistemas de información o cuando es requerido un mantenimiento a aplicaciones que se encuentren en funcionamiento.

1. Seguridad

- ☑ Las especificaciones iniciales de seguridad en relación con los accesos de los usuarios a las aplicaciones se efectuarán durante la fase del diseño lógico del ciclo de vida de sistemas. Tal especificación debe ser definida por el Jefe de Área o funcionario responsable de esta actividad.
- ☑ La creación o modificación de los accesos a bases de datos, tablas, vistas o campos particulares es función del DBA o funcionario responsable de la administración de los datos de la compañía. Esta actividad tendrá como soporte el formato “Solicitud de Acceso” y que debe ser diligenciado por el área usuaria en el diseño de la aplicación o mediante actualizaciones requeridas.
- ☑ Para cada base de datos o tabla que se cree, deberá definirse con el usuario si se requiere un “Log transaccion” o “audit trail”. La determinación se hará con base en la criticidad de la información que se maneje.

- Al momento de entregarse una aplicación en bases de datos a producción, deberá ser revocada la propiedad que tiene el analista sobre la base de datos y asignar los derechos propios de los usuarios de la aplicación.
- La asignación de frecuencias automáticas en los cambios de los passwords la hará el jefe del Area Usuaría, indicando este dato en el formato de "Solicitud de claves de acceso".
- La gestión de actualización a la seguridad lógica de los datos de la CAC se adelantarán por medio de una base de datos en la cual se consignen los usuarios de la base de datos con los respectivos derechos a nivel de bases, tablas y campos relacionados. A esta base de datos tendrán acceso los jefes de área para consultar información relacionada con los privilegios que evidencian los datos antes de proceder a autorizar nuevos derechos de accesos solicitados internamente o desde otras áreas usuarias.
- La asignación de seguridad para las bases de datos, para las tablas y para campos deberá hacerse solo desde el sistema manejador de bases de datos.
- Todos los datos contenidos en las bases de datos deben tener un período de retención definidos, para efectos de programar depuraciones y almacenar solo la información realmente necesaria. Esta definición es establecida por parte de los usuarios administradores de dicha información conforme a las normas de la compañía y a las disposiciones legales.
- Los procesos desarrollados en la base de datos serán registrados en una bitácora en la cual se detallen las operaciones de interés tales como copias de seguridad, reorganización de índices, reinicios del sistema, aplicación de programas diagnóstico o utilitarios, etc.

2. Producción

- Las bases de datos existentes en la compañía tendrán un período de retención definido. Tal retención permitirá depuraciones periódicas de las tablas en producción como en dispositivos de backups.
- El procesamiento en bases de datos dispondrá de equipos de respaldo fuera de la CAC mediante convenios con otras compañías afines en el hardware que se tenga instalado.
- Las bases de datos deberán ser sometidas a depuraciones periódicas por parte de los usuarios responsables.

3. Desarrollo

- Las aplicaciones desarrolladas en la empresa tendrán un diccionario de datos en el cual se detallen los elementos de las tablas con base en los diccionarios de datos que generan los analistas durante el diseño de la información.
- Las aplicaciones desarrolladas en ambientes de cuarta generación deberán poseer carpetas de programas, manuales de usuario, operador y técnico, conservándose copia magnética en el centro de documentación (librería o biblioteca) de sistemas.

- La distribución de las bases de datos de una aplicación en los volúmenes disponibles será previamente definidas por el funcionario encargado de la administración de los datos de la compañía.

No. 5. POLÍTICAS PARA LA ADMINISTRACIÓN DE LOS RECURSOS TECNOLÓGICOS DE UNA CAC

Las políticas son la base fundamental de todo esfuerzo enfocado a la seguridad de la información. Con el fin de ser efectivo, el proceso para fortalecer la seguridad de la información debe tener un conjunto de políticas que brinden instrucciones claras y establezcan el soporte de la alta gerencia. Las políticas son usadas como punto de referencia para un sinnúmero de actividades relacionadas con la seguridad de la información tales como: Diseño de controles en los sistemas de información, controles de acceso, análisis de riesgos, investigaciones de crímenes por computadora, y sanciones disciplinarias de funcionarios por violaciones en la seguridad.

Como las políticas de seguridad tienen un impacto muy alto en la organización, es muy importante que estas sean claras, concisas y que respondan al ambiente donde se pretenden implementar. Las políticas deben ser revisadas periódicamente para asegurar su aplicabilidad en la organización. El propósito de esta directriz es asesorar a los funcionarios que están desarrollando las políticas por primera vez o revisándolas.

A continuación se ofrece una guía práctica y puntual al complejo proceso de desarrollar políticas de seguridad en informática.

Nota: Entre otras cosas dentro de este proceso se debe obtener la aprobación de la alta gerencia, divulgarlas y generar controles que permitan hacer seguimiento a su efectividad y aplicación.

ASPECTOS A TENER EN CUENTA

1. ORGANIZACIÓN

Políticas:

- Debe existir un comité de sistemas (informática), conformado por funcionarios de áreas de administración, que será el encargado de avalar los requerimientos de hardware o software de la CAC.
- Se debe asignar presupuesto por área, para todo lo que tiene que ver con recursos de informática.

Compras, cambios o eliminaciones de elementos de software o hardware.

Políticas:

- El comité de sistemas será el encargado de la administración de recursos de hardware y software.
- Todo requerimiento de hardware o software debe pasar a estudio por el comité de sistemas.
- Toda compra de hardware o software debe estar soportada por lo menos de tres (3) cotizaciones, bajo los mismos términos de referencia.

- Toda eliminación de recursos de informática, debe ser reportada por el director de área y pasar a comité de sistemas.
- Toda compra debe estar soportada por pólizas de cumplimiento.
- Todo elemento de software o hardware debe tener contrato de mantenimiento.

Las justificaciones de nuevas adquisiciones.

Políticas:

- Todo requerimiento de hardware o software debe tener adjunto, los términos de referencia a evaluar.
- Se debe contar con el presupuesto asignado para recursos de informática.

Alternativas manuales que garanticen normal desempeño.

Políticas:

- Debe existir plan de capacitación a funcionarios del área de informática.
- Deben existir manuales de procedimientos para cada proceso de la CAC.
- Debe existir manual de operación para cada uno de los aplicativos de la compañía.
- Se debe contar con formatos prenumerados que garanticen el desarrollo manual de cualquier actividad.
- Se deben realizar inventarios generales de elementos de hardware y software de manera periódica.

Difusión de políticas.

Políticas:

- El documento que contiene la política de seguridad debe ser difundido a todo el personal de la CAC.
- Toda política debe seguir un proceso de actualización y seguimiento.

Respaldo técnico y garantía tecnológica.

Políticas:

- Todo contrato, ya sea de adquisición o mantenimiento de elementos de informática, se debe llevar a cabo con compañías debidamente legalizadas.
- Se debe contar con cronograma de mantenimiento a dispositivos de la red.
- Se debe contar con plan de copias de seguridad (backups).
- Todo software o hardware debe contar con sus respectivos manuales técnicos.

La capacitación y entrenamiento a usuarios de computadores.

Políticas:

- Se debe contar con plan de capacitación en nuevas tecnologías a funcionarios de sistemas.
- Se debe contar con planes de capacitación a nuevas versiones del software instalado en la CAC.

- Se debe contar por lo menos con un Help Desk dentro de la compañía.
- Toda capacitación patrocinada por la CAC debe ser retroalimentada a las áreas que lo ameriten.

2. SOFTWARE

Propiedad Intelectual

Políticas:

- Todo programa adquirido por la CAC será propiedad de esta y mantendrá los derechos de propiedad intelectual que este posea.
- El departamento de informática es el responsable de realizar revisiones periódicas a los equipos para que solo exista software licenciado en las instalaciones de la compañía.
- Corresponde a la dirección de informática autorizar cualquier compra o actualización del software.
- Todo software de dominio público vendrá de sitios seguros.

Desarrollo de software de acuerdo a la metodología de desarrollo existente.

Políticas:

- El área de informática emitirá las normas y procedimientos para instalación de software básico en todo tipo de equipo.
- El área de informática será la responsable de brindar asesoría y supervisión para la instalación de nuevo software.
- Todo software que desde el punto de vista del área de informática coloque en riesgo los recursos de la compañía no es permitido.

Desarrollos de sistemas soportados en micros y su documentación.

Políticas:

- Todo procedimiento que en buen uso de la información se desarrolle bajo software ofimático debe estar debidamente documentado.
- Es responsabilidad de cada área informar al departamento de informática sobre rutinas o desarrollos que se generen en el área.
- Se deben respetar los derechos de autor para cada desarrollo en particular que ayude al normal funcionamiento de sus labores.

Revisión de Auditoría

Políticas:

- El área de auditoría debe ser la responsable de dar cabal cumplimiento a cada una de las políticas establecidas.
- El comité de sistemas debe contar con la participación activa de un funcionario de auditoría.
- Se deberá dar cumplimiento a cada uno de los requerimientos que plantee la auditoría.

3. HARDWARE

Políticas:

- Criterios de compatibilidad con la base instalada de equipos de la CAC.
- Compartir al máximo los recursos, definiendo restricciones de seguridad.
- Inventario periódico.
- Cambios de localización, apertura y mantenimiento de equipos.
- Uso de equipos especiales.
- Solicitud de disquetes, cintas, CD o medios afines.

4. USUARIO

Políticas:

- Toda solicitud de programas o equipos de acuerdo con los procedimientos de compras de la empresa.
- Responsabilidad de la correcta administración de la información que utilice, previendo las acciones de seguridad y confidencialidad.
- identificador individual de acceso.
- Espacio en disco duro del servidor. Invasión de áreas de disco asignadas a otros usuarios.
- Área del disco servidor destinada para el sistema operacional, programas de aplicación o utilitarios.
- Prohibición al uso de cualquier tipo de software que no esté autorizado por la CAC.

5. ÁREA DE SISTEMAS

Políticas:

- Atención a usuarios de manera continua y segura.
- Continuidad en el procesamiento y la reducción de tiempos.
- Espacio en disco necesario para almacenamiento de datos.
- Garantizar la permanencia fiel de los datos que residan en discos del servidor.

No. 6. AUDITORIA A LOS MICROCOMPUTADORES Y REDES LAN

Se relacionan a continuación algunas preguntas que son pertinentes al momento auditar una red de microcomputadores. Se evalúan los siguientes aspectos:

1. Políticas administrativas.
2. Adquisición de hardware.
3. Adquisición y desarrollo de software.
4. Documentación.
5. Comunicaciones.
6. Entrenamiento y soporte a usuarios.
7. Mantenimiento.
8. Seguros.
9. Seguridad.
10. Procedimientos de respaldo.

PRUEBAS A REALIZAR POR CADA ASPECTO

1. POLÍTICAS ADMINISTRATIVAS:

- Verificar la existencia de políticas administrativas escritas para:
 - Adquisición de microcomputadores.
 - Uso de microcomputadores.
 - Verificar si se mantiene una lista actualizada de todos los usuarios de microcomputadores.
 - Verificar la existencia de un grupo de trabajo o comité para coordinar los proyectos desarrollados en micros.
- Evaluar los medios de difusión periódica de nuevos desarrollos.

2. ADQUISICIÓN DE HARDWARE

- Verificar la existencia o respaldo, con análisis de costo-beneficio, de las solicitudes de compra de equipos por parte del usuario.
- Evaluar la documentación existente para el hardware.
- Se hace una planeación del sitio en que se instalaron los equipos para garantizar:
 - Protección antimagnética.
 - Servicio eléctrico regulado.
 - Conexión a la red.
 - Seguridad física.
- Evaluar la memoria RAM del servidor, frente al número de usuarios que posee.
- Evaluar la capacidad del disco duro del servidor, con relación al número de usuarios.
- Revisar el registro de uso de microcomputadores para cada área usuaria.

3. ADQUISICIÓN DE SOFTWARE

- Verificar la existencia de políticas para uso y adquisición de software.
- Obtener una lista de las versiones de paquetes en uso, en los diferentes micros. Verificar que sean copias originales y licenciadas por la CAC
- Verificar la existencia de alternativas manuales, para llevar a cabo las tareas que actualmente se procesan en micros.
- Revisión de archivos en el disco del servidor.
- Verificar la existencia de un plan general sobre los desarrollos propuestos por los usuarios.

4. DOCUMENTACIÓN

- Verificar la existencia de un catálogo actualizado del software aplicativo, desarrollado y adquirido por la CAC.
- Verificar la existencia de una metodología de desarrollo para micros.
- Evaluar la documentación requerida para aplicaciones desarrolladas en microcomputadores.

5. COMUNICACIONES

Tomando como base los 7 niveles de red de la ISO verificar:

Nivel 1. Físico

- Evaluar el plano de la red, con base en los siguientes aspectos:
 - Dispositivos adjuntos.
 - Diagramas del cableado.
 - Documentación.
 - Actualización.
- Verificar la existencia de procedimientos para mantenimiento periódico.
- Analizar el soporte de proveedores alternos, si el proveedor falla.
- Verificar la existencia de procedimientos para recuperación de fallas.

Nivel 2: De enlace de datos

- Verificar si existe un monitoreo de transmisiones y determinar si:
 - Es continuo o esporádico.
 - Existen tasas de estadísticas de errores.
 - Se investigan altas tasas de error.

Nivel 3: De redes

- Verificar las estrategias para monitoreo de las tasas de tráfico de la red.
 - Verificar la existencia de tablas de ruta de la red.
 - Efectuar revisión a estadísticas de tráfico.
 - Verificar el aprovechamiento de las herramientas que provee el sistema operativo: Ejemplo en Windows 2000
 - Monitor de eventos - EventViewer Manejo de su tamaño, copias.
 - Monitor del sistema – Programas, procesos y desempeño.

- Optimización del desempeño. Uso de contadores de uso de memoria, procesador.
- Uso de alertas.
- Manejo de espacio en disco.
- Servicios instalados del servidor.
- Verificar la conectividad a Internet en cuanto a:
 - Controles de acceso a Internet.
 - Firewall
 - Proxy
 - DNS
 - DHCP

- Uso de correo electrónico, administración del servicio, definición de usuarios etc, tamaños de adjuntos.
- Administración del Antivirus

Nivel 4: De transporte

- Establecer los actuales procedimientos para iniciar la red después de:
 - Instalación inicial.
 - Falla o modificación.
 - Operación diaria.
- Evidenciar la capacidad para detectar errores y corregirlos en transmisiones fin a fin:
 - Monitoreo.
 - Estadísticas.
 - Investigación de alzas.
- Establecer si son adecuados los controles de acceso a las tablas del sistema operacional de la red.
- Verificar la existencia de un registro automático diario o huella de Auditoría para los cambios a las tablas.
- Verificar la existencia de backups de las tablas del sistema operacional.

Nivel 5: De sesión

Verificar para cada estación de trabajo y para el servidor de la red si:

- Se puede acceder el sistema operacional.
- Las claves de acceso son:
 - Usadas adecuadamente.
 - Compartidas.
 - Cambiadas periódicamente.
 - Cambiadas cuando el personal es transferido.
 - Requeridas para todas las estaciones de la red.
 - Requeridas por el sistema operacional de la red.
- Establecer si existe un procedimiento para recuperación de claves de acceso.
- Verificar si existe un procedimiento de control para claves de acceso, a la red de microcomputadores.

- Determinar si el sistema operacional de la red o cualquier programa monitor controla:
 - Las actividades realizadas en cada estación de trabajo.
 - Las violaciones de acceso realizadas por estación de trabajo.
- Determinar si los controles de acceso para tablas de seguridad son adecuados.
- Verificar que las tablas de seguridad sean respaldadas frecuentemente y almacenadas fuera del sistema.
- Verificar si existe una huella de Auditoría o un registro automático diario, para todos los cambios hechos sobre las tablas de seguridad.

Nivel 6: De presentación

- - Determinar si existe criptografía y establecer:
 - Si es por software.
 - Si es por hardware.
 - Cuantas claves se usan.
 - Si suministran seguridad apropiada.
 - Si las claves son cambiadas y con qué frecuencia.

Nivel 7: De aplicación

- Pruebas para diagnóstico de la seguridad:
 - Establecer si las aplicaciones son individualmente seguras.
 - Verificar la existencia de limitaciones por clase de transacción, para determinados usuarios.
 - Verificar las restricciones establecidas para cada nivel de acceso diferente.
 - Establecer si existe algún seguimiento para actividades inválidas.
 - Establecer si el analista de la red es avisado de la violación y si éste avisa a los usuarios involucrados.
 - Establecer si se hace seguimiento al caso anterior.
 - Establecer si se usan archivos para pistas de Auditoría, disco o servidor para respaldo.
 - Establecer si existe un procedimiento para ayudar a los usuarios en la recuperación.
 - Establecer si hay alguien más responsable para el respaldo del servidor.
 - Establecer si existe un procedimiento definido para backups.
- Pruebas para diagnóstico de las aplicaciones:
 - Verificar la revisión del software, antes de instalarse definitivamente en las Áreas de Producción.
 - Revisar los sitios de almacenamiento de la documentación sensible, cuando no está en uso.
 - Verificar si son usadas versiones de red (actualizadas) de programas de aplicación.
 - Verificar si hay violación de área entre los usuarios.

6. ENTRENAMIENTO Y SOPORTE A USUARIOS

- Verificar la existencia de un programa de capacitación definido, para los usuarios en hardware y software.

- Verificar la existencia de material para auto estudio.
- Establecer si se incluye en la capacitación a los usuarios, la difusión de normas y políticas establecidas por la empresa con respecto a los micros.
- Establecer si se efectuaron análisis de necesidades de capacitación de los usuarios.

7. MANTENIMIENTO

- Evaluaciones de los contratos de mantenimiento actuales.
- Verificar la existencia de un programa para el mantenimiento preventivo y si existe, averiguar si lo conocen los usuarios y cómo se controla.
- Establecer si existe un control que relacione los números de serie de las partes de los equipos que son llevados a mantenimiento a otras empresas.
- Establecer si existe un procedimiento a seguir en caso de daño de un equipo y si existe, verificar si lo conocen los usuarios.
- Establecer si se ha dado instrucciones al personal de limpieza, cuando éste se encuentra en un área de micros.
- Establecer qué tipo de interventoría tiene la gestión de los contratistas.
- Establecer si se protegen con forros plásticos el teclado, la pantalla y CPU.
- Revisar cuál es el tipo de mantenimiento.
- Establecer si existe un programa de las actividades del mantenimiento preventivo del contratista.

8. SEGUROS

- Verificar si se tienen pólizas de seguros que amparen los microcomputadores.
- Verificar si las estipulaciones de las cláusulas corresponden con las instalaciones físicas de los micros (tarjetas, velocidad, valor, etc.)
- Revisar los procedimientos de reporte a la aseguradora con respecto a los eventos ocurridos con los equipos.

9. SEGURIDAD

- Seguridad del hardware:
 - Verificar si se tiene un registro de todos los números seriales de los equipos periféricos y sus partes más relevantes (tarjetas especiales).
 - Verificar si se hacen comparaciones periódicas entre el inventario físico y el registro.
 - Verificar si están los microcomputadores ubicados en áreas de tráfico limitado.
 - Confirmar si se tiene seguridad, para verificar cuando un equipo ha sido destapado sin autorización.
- Seguridad del software:
 - Verificar si se tiene establecido el procedimiento para autorización de nuevos usuarios.
 - Verificar si se tienen identificados los archivos de datos confidenciales.
 - Verificar si se registra el acceso y uso de los equipos.

- Verificar si se tienen identificados, para cada aplicación, los archivos que deben mantenerse residentes en el disco duro.

10. RESPALDO DE EQUIPOS Y PERIFÉRICOS

- Verificar si existen procedimientos definidos para el uso de otros equipos, en caso de fallas prolongadas.
- Verificar si se tienen procedimientos manuales documentados, en caso de que el procedimiento no pueda ser realizado en el microcomputador.
- Verificar si se tienen identificadas las prioridades a seguir, en caso de daños en los equipos.
- Revisar si se utilizan programas de utilidad aprobados, para recuperar datos en medios destruidos.