# CAPÍTULO IV
# 4. AUDITORÍA DE SISTEMAS

## 4.1 INTRODUCCIÓN

El nivel académico en armonía con la tecnología, la capacidad y experiencia son elementos importantes para el buen desarrollo de la auditoría en TI, asimismo el responsable de ejecutar la evaluación debe considerar escenarios de posibles "supuestos" que permitan ampliar o profundizar las pruebas para minimizar los riesgos, por ello el proceso de auditoría exige que el auditor de TI reúna evidencia, evalúe fortalezas y debilidades de los controles existentes, y que prepare un informe de auditoría que presente esos temas en forma objetiva a la Administración o Gerencia de la cual depende. Asimismo el auditor debe ser portador de independencia y autoridad para realizar su examen.

Como primer paso, la planificación es necesaria para realizar auditorías de TI. El auditor debe comprender el ambiente del negocio en el que se ha de realizar la auditoría, así como los riesgos del negocio y control asociado. Por ello el auditor antes de aplicar los programas de trabajo debe tener en cuenta las siguientes consideraciones.

Al planificar una auditoría, el auditor de TI debe tener una comprensión suficiente del ambiente total que se revisa, debe incluir una idea general de las diversas prácticas comerciales y funciones relacionadas con el tema de la auditoría, así como los tipos de sistemas que se utilizan. El auditor de TI también debe comprender el ambiente normativo en el que opera el negocio.

## 4.2 PERFIL DEL AUDITOR DE SISTEMAS Y NORMAS BÁSICAS DE APLICACIÓN

Cada empresa tiene establecido los criterios, condiciones y obligaciones que deben ser respetados por el personal que labora en ella, esto obedece a que son aspectos vigentes que regulan la actuación de quienes administran la empresa, por tanto, es compromiso del auditor apegarse a las normas o políticas establecidas, sean estas

internas o externas en el ejercicio del servicio profesional, auditoria de sistemas debe de exigir el cumplimiento de normas básicas o principios generales aceptados.
En cualquier ámbito laboral existen necesidades que cumplir, el primer requisito que debe poseer quien se dedica a esta profesión, es estar totalmente libre de cualquier tipo de influencia; es decir debe ser autónomo en su actuación y no permitir ningún tipo de injerencia, ya sea de cualquier carácter, sean estas; laborales, morales, conducta, independencia y conocimiento profesional. El segundo requisito son los conocimientos computacionales que debe tener, con un amplio cúmulo de nociones en áreas vinculadas al trabajo, métodos, herramientas y técnicas de auditoría a fin de que pueda realizar sus tareas con eficiencia y eficacia.

Sin embargo, este debe poseer otras características personales que son representativas del auditor tales como: honradez, valores, confianza, tenacidad, capacidad analítica, en ese contexto también lo ideal es la experiencia profesional para el buen desempeño del trabajo dentro de la Organización. Así mismo debe el auditor de sistemas manejar otros factores que contribuyen y se encuentran ligados a su profesión, tales como: a) El auditor debe de aprender a manejar adecuadamente las relaciones personales, profesionales y laborales entre él y el auditado. b) Como profesional de auditoría debe utilizar la misma metodología, procedimientos, herramientas y técnicas que se hayan establecido para la revisión de las áreas. c) Los resultados que obtiene el auditor forman evidencias en las que se respalda, para emitir el dictamen .d) Es obligación profesional, moral y personal del auditor respetar la confidencialidad de dicha información y no divulgarla. d) Mantener y aplicar la equidad, en virtud que trata de igualar la justicia, ponderación y emisión de juicios; la imparcialidad que evita las preferencias injustas y la razonabilidad que es la capacidad del individuo para emitir un juicio.

La sociedad misma identifica una serie de aspectos fundamentales que debe de tener el profesional dedicado a la auditoría, a fin de que identifique y cumpla con los principios y valores del auditor, citando algunos de ellos:

### 4.2.1 INDEPENDENCIA

La independencia supone una actitud mental que permite al auditor actuar con libertad respecto a su juicio profesional, para lo cual debe encontrarse libre de cualquier predisposición que limite su imparcialidad en la consideración objetiva de los hechos, así como en la formulación de sus conclusiones.
Para ser independiente, el auditor no debe tener intereses ajenos a los profesionales, ni estar sujeto a influencias susceptibles de comprometer tanto la solución objetiva de los asuntos que le son sometidos, como la libertad de expresar su opinión profesional.

### 4.2.2 INTEGRIDAD

La integridad debe entenderse como la rectitud intachable en el ejercicio profesional, que le obliga a ser honesto y sincero en la realización de su trabajo y en la emisión de su informe. En consecuencia, todas y cada una de las funciones que realice han de estar regidas por una honradez profesional irreprochable.

### 4.2.3 OBJETIVIDAD

La objetividad implica el mantenimiento de una actitud imparcial en todas las funciones del auditor. Para ello, debe gozar de una total independencia en sus relaciones con la entidad auditada. Debe ser justo y no permitir ningún tipo de influencia o prejuicio.

### 4.2.4 COMPETENCIA PROFESIONAL

Es la obligación de mantener su nivel de competencia a lo largo de toda su carrera profesional, así como de mantener sus conocimientos y sus habilidades a un nivel adecuado para asegurar que la evaluación será la adecuada.

### 4.2.5 CONFIDENCIALIDAD

El Auditor deberá respetar la confidencialidad respecto a la información que reúna en el desarrollo de su trabajo y no deberá revelar ninguna información a terceros sin la autorización específica, a menos que tenga el derecho o la obligación profesional o legal de hacerlo. También tiene la obligación de garantizar que el personal bajo su control respete fielmente el principio de la confidencialidad.

El principio de confidencialidad es más amplio que la revelación de la información; incluye el hecho de que un auditor que obtenga información en el curso de la prestación de sus servicios, no debería usarla ni aparentar usarla para su beneficio personal o para terceros.

### 4.2.6 RESPONSABILIDAD

Se mantiene como responsabilidad el hecho de aceptar el compromiso que implica la toma de decisiones y las consecuencias previstas por las acciones y omisiones en el cumplimiento del trabajo.

### 4.2.7 CONDUCTA PROFESIONAL

Actuar de acuerdo con la buena reputación de la profesión y evitar cualquier conducta que pueda desacreditarla. Esto requiere que las normas de ética tengan en cuenta las responsabilidades profesionales.

### 4.2.8 NORMAS TÉCNICAS

El auditor deberá conducir una auditoría conforme las Normas y Políticas, locales o internacionales. Estas deberán contener principios básicos y procedimientos esenciales junto con lineamientos relativos y asociados a las funciones del auditor.

Los elementos referenciados con anterioridad se encuentran integrados en normas llamadas código de ética, aplicadas para el auditor de sistemas, siendo estos utilizados y difundidos por instituciones nacionales e internacionales. (Anexo E)

## 4.3 RIESGO Y MATERIALIDAD DE AUDITORÍA

Se pueden definir los riesgos de auditoría como aquellos riesgos en que la información pueda tener errores materiales o que el auditor de TI no pueda detectar un error que ha ocurrido. Los riesgos en auditoría pueden clasificarse de la siguiente manera:

- **Riesgo inherente:** Cuando un error material no se puede evitar que suceda por que no existen controles compensatorios relacionados que se puedan establecer.
- **Riesgo de control:** Cuando un error material no puede ser evitado o detectado en forma oportuna por el sistema de control interno.
- **Riesgo de detección:** Es el riesgo en que el auditor realiza pruebas exitosas a partir de un procedimiento inadecuado. El auditor puede llegar a la conclusión de que no existen errores materiales cuando en realidad existen. La palabra "material" utilizada con cada uno de estos componentes o riesgos, se refiere a un error que debe considerarse significativo cuando se lleva a cabo una auditoría.

En una auditoría de TI, la definición de riesgos materiales depende del tamaño o importancia del ente auditado, así como de otros factores. Una auditoría tal vez no detecte cada uno de los potenciales errores en el universo. Pero, si cuando el tamaño de la muestra es lo suficientemente grande, o se utiliza procedimientos estadísticos adecuados se llega a minimizar la probabilidad del riesgo de detección. De manera similar al evaluar los controles internos, el auditor de TI debe percibir que en un sistema dado, se puede detectar un error mínimo, pero ese error combinado con otros, puede convertirse en un error material para todo el sistema.

Aunque siempre debe prevalecer el deber del secreto profesional del auditor, conviene recordar que en el caso de detectar fraude durante el proceso de auditoría

procede actuar en consecuencia con la debida prudencia que aconseja, sobre todo si afecta a los administradores de la organización. Ante un caso así, conviene consultar con la Alta Administración o el Comité creado para tal fin, así mismo con el asesor jurídico, e identificar leyes afines para tal efecto, por ejemplo: Código Penal, Código Civil, Código de Comercio, Ley de Propiedad Intelectual y otras disposiciones. Al determinar qué áreas funcionales o temas de auditoría deben auditarse, el auditor puede enfrentarse ante una gran variedad de temas, por ello debe evaluar esos riesgos y determinar cuales de esas áreas de alto riesgo deben ser auditadas.

### 4.3.1 EVIDENCIA

La evidencia es la base razonable de la opinión del Auditor de TI, esto es parte complementaria del Informe, la evidencia tiene una serie de calificativos:

- La evidencia relevante, que tiene una relación lógica con los objetivos de la Auditoría.
- La evidencia fiable, que es válida y objetiva, aunque con nivel de confianza.
- La evidencia suficiente, que es de tipo cuantitativo para soportar la opinión profesional del auditor.
- La evidencia adecuada, que es de tipo cualitativo para afectar a las conclusiones del auditor.

## 4.4. HERRAMIENTAS DE SOPORTE

### 4.4.1 SOFTWARE PARA AUDITORÍA

EL auditor de sistemas puede auxiliarse con herramientas alternas que existen en el medio creadas para dicho fin, por ejemplo: para evaluar las Bases de Datos, estas permiten medir la consistencia, coherencia y calidad de los datos, para evaluar redes; estas permiten monitorear la seguridad y la continuidad del servicio. Al respecto podemos mencionar algunas de ellas:

#### 4.4.1.1 ACL

ACL es un software para la solución de auditoría y análisis de datos, siendo su significado “Lenguaje de Control para Auditoría”, es un producto reconocido en el mundo por su excepcional servicio y soporte técnico, siendo un valor agregado para las empresas por sus ventajas de generación de reportes que se almacenan como papeles de trabajo. El software es un producto eficiente según las características siguientes:

a) Funcionalidad incorporada para; auditar y analizar datos mediante poderosos comandos tales como: estratificar, muestreo y duplicados.
b) Facilidad para el análisis interactivo; aplicando cualquier metodología de auditoría, analizando sus datos de forma que los resultados son inmediatos no importando la cantidad de registros que contenga el archivo, por su manejo de alta capacidad y velocidad en el proceso.
c) Facilidad de uso; su interfaz amigable que incluye facilidades como: menús, barras de herramientas y comandos.
d) Análisis universal de datos; una vez que se accede los datos, ACL los puede leer en su formato nativo, utilizando un solo producto en una herramienta para leer cualquier plataforma tecnológica, incluyendo bases de datos que cumplan con las especificaciones de ODBC, archivos de longitud variable, archivos de texto y muchos mas.
e) Procesamiento de varios archivos; trabaja simultáneamente con varios archivos, para hacer análisis y reportes mas complejos.
f) Identifica tendencias y señala excepciones y áreas que requieren atención.
g) Localiza errores y posibles irregularidades, comprobando y analizando los datos según los criterios del auditor.
h) Verifica integridad de datos en los archivos.
i) Emite cálculos estadísticos y analíticos para realizar proyecciones.
j) Despliegue de Gráficos de Barra

#### 4.4.1.2 IDEA

Datos Interactivos Extracción y Análisis (IDEA) es una herramienta para auditores, contadores y administradores financieros que necesitan auditar, revisar, analizar, extraer y evaluar información contenida en sistemas, base de datos y cualquier archivo electrónico.

Este software permite la ejecución de procesos como consultas a archivos de datos, calcular totales o promedios, encontrar cuantas transacciones o registros cumplen un criterio dado o buscar campos inusuales. La interfaz del software está orientada hacia los usuarios finales, de manera que su uso y aplicación resulta amigable con el usuario, el software presenta algunas características:

a) Análisis de información: IDEA permite realizar una serie de funciones de análisis sobre los datos extraídos, mejorando la confianza y la exactitud de la información utilizada por el auditor.
b) Ordenamiento de registros: IDEA permite ordenar registros hasta por ocho llaves de ordenamiento concatenado, ascendente o descendente.
c) Gráficos de barra: permite visualizar de modo gráfico la información que está analizando.
d) Estadísticas de un campo: muestra una variedad de información estadística de un campo numérico y puede actuar hasta para 32 campos Simultáneamente.
e) Comparación de dos archivos: permite comparar dos archivos similares e identificar eventuales diferencias entre ambos.
f) Detección de errores de secuencia: permite detectar errores de secuencia en un archivo, como por ejemplo en un archivo de cheques emitidos.
g) Detección de llaves duplicadas: permite detectar campos duplicados que deberían ser únicos.

#### 4.4.1.3 TEAM-MATE

Es un software que dispone de un sistema administrador de usuarios de la Base de Datos, de manera que cada usuario tiene diferentes niveles de acceso. Está diseñado para ser utilizado por todos los sectores, comerciales, industriales, financiero; así como para todo tipo de auditoría, como financiera, de cumplimiento, procedimientos, operacionales, investigaciones y auditoría de TI, dispone de integrar el programa de auditoría con las observaciones o comentarios afines para luego poderlo relacionar al papel de trabajo no importando su formato, ello le permite la flexibilidad y manejo operativo del mismo. También dispone de módulo de evaluación de riesgos, basada en la metodología ORCA (Objetivos, Riesgos, Controles y Alineación), esta enfocada en cómo una organización, unidad de negocio, proceso de negocio o individuo define y prioriza sus estrategias y objetivos. La metodología ORCA determina el impacto del riesgo en el objetivo y su probabilidad de ocurrencia. También dispone de Team Risk el cual permite la evaluación de riesgos, determinando el universo de riesgo con objetivos y controles que pueden ser editados durante el proceso de evaluación. Team Risk permite determinar la fórmula de puntuación y las bandas de puntuación (scoring), las métricas de puntuación, como impacto y probabilidad que mejor describan su forma de determinar el riesgo, las dimensiones de las métricas para ver los factores de riesgo antes y después del control o ambos.

#### 4.4.1.4 MAGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (MAGERIT). Está compuesto por: Aproximación a la Seguridad de los Sistemas de Información, Procedimientos, Técnicas, Desarrolladores de Aplicaciones, Responsables del Dominio, Legales y Técnicas, Arquitectura de la Información y especificaciones de la interfaz para el intercambio de datos.

El modelo normativo de MAGERIT se apoya en tres sub modelos: Componentes, Eventos y Procesos, la metodología permite estudiar los riesgos que soporta un sistema de información y el entorno asociado a él, por ello propone la realización de

un análisis de los riesgos que implica la evaluación del impacto que una falta en la seguridad que tiene la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

Los Criterios de Seguridad de normalización y conservación recogen los requisitos y recomendaciones relativos a la implantación de las medidas de seguridad organizativa y técnica para asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en el diseño, desarrollo, implantación y explotación de las aplicaciones que la Administración General del Estado utiliza para el ejercicio de sus potestades. Estos criterios pueden ser, por tanto, complemento de MAGERIT para la identificación y selección de funciones y mecanismos de salvaguarda.

En cuanto al derecho de utilización, MAGERIT es una metodología usada por el Gobierno Español y es de carácter público, perteneciente al Ministerio de Administraciones Públicas. Su utilización requiere autorización previa del MAP. MAGERIT es una opción para poderse aplicar en el sector gubernamental y por consiguiente con algunas adaptaciones conforme a las leyes del país.

#### 4.4.1.5 OTROS

Para el monitoreo, seguimiento y control de Base de Datos puede auxiliarse por ejemplo de Spotlight el cual permite operar en tiempo real, identifica problemas de entrada y salida, mantiene historia y relaciones de hechos, realiza calibraciones de la base, alarmas audibles , tiempo y espacio de cpu, disponibilidad de memoria principal, disponibilidad de discos, tiempo y espacio de procesos, otra opción de software es NimBUS que se utiliza para monitorear bases de datos e indica la disponibilidad y rendimiento de los servidores de bases de datos. Además, soporta múltiples plataformas de bases de datos: Oracle, Sybase, DB2, MS SQL, e Informix. Otras características*:* evalúa clusters de bases de datos, bitácoras de eventos, usuarios activos, consumo de recursos, opciones flexibles de notificación de alarmas

(SMS, PDA, consola, web, email, etc) alertas e indicadores de rendimiento, análisis de entradas en tablas para la generación de alertas e informes de tendencia, entre otros.

Por otra parte conforme al conocimiento del auditor y la plataforma tecnológica con la que cuenta la Organización, el auditor de sistemas puede apoyarse con software de soporte para el desarrollo de sus evaluaciones, por ejemplo: Visual Fox, Visual Basic, Sql, e inclusive los procedimientos definidos en la línea de comandos de un AS-400 ó cualquier otro lenguaje que le permita filtrar, definir, seleccionar y evaluar los datos, con la finalidad de brindar opinión sobre la calidad, coherencia y existencia de la información almacenada.

Así mismo se recomienda que el auditor pueda identificar aquellos procedimientos o consultas que demanden la creación de sentencias o líneas de código fuente, sabiendo que estas se utilizarán más de una vez, en el sentido que le permita disponer de un respaldo de los mismos, para que en futuras evaluaciones sean ejecutados.

## 4.5 SOFTWARE DE MONITOREO PARA REDES

La seguridad se hace posible con el desarrollo de negocios a través de Internet y debe ser un componente fundamental de cualquier estrategia de comercio electrónico. A medida que las empresas abren sus redes a más usuarios y aplicaciones, las exponen a mayores riesgos. Por ello las organizaciones o personas que comparten información y que ingresan con sus equipos a una red por cualquier clase de motivo, es prácticamente imprescindible usar algún Corta Fuego (Firewall) y de herramientas que le permitan monitorear la red, sobre todo sí comparte archivos a través de Internet, utiliza un servidor Web, utiliza algún tipo de herramienta de control remoto como PC Anywhere, Laplink o Servicios de Terminal de Microsoft o desea estar protegido ante ataques de denegación de servicio (DoS) o intrusiones. Al respecto presentamos a manera de ejemplos algún software que pueden servir de soporte para ejercer auditoría en las redes de comunicaciones:

| SOFTWARE | DESCRIPCION |
|---|---|
| CISCO | Dispone de una variedad de productos para la seguridad y confiabilidad del servicio de red. |
| DEFENDER | Es un sistema contra hacker, explora el DSL, módem de cable, o conexión de marcado manual del Internet que busca actividad del hacker. Cuando detecta una intrusión, bloquea automáticamente el tráfico de esa fuente, evitando a intrusos tener acceso a su sistema. Tiene como punto fuerte combinar dos programas de seguridad en uno, un Firewall y un Analizador de red. El Firewall funciona de la misma manera que la mayoría de Firewall, bloquea o permite el tráfico según las preferencias del usuario, y el analizador de red intenta determinar la naturaleza de los paquetes. |
| DTK | (ToolKit) es una caja de herramientas de engaño diseñada para dar ventaja a los usuarios propietarios, para dar órdenes de engaño a los atacantes. |
| ETHEREAL | Es un sistema capaz de obtener datos de múltiples Sniffers de sistema, desde ficheros o directamente de la red. En este último caso, puede ser usado en redes de tipo Ethernet, FDDI, PPP, Token-Ring, IEEE 802.11, IP sobre ATM e interfaces de loopback. Con este analizador se puede diseccionar a más de 700 protocolos de red, pudiendo guardar la información obtenida en ficheros, así como filtrar la información mostrada en pantalla. |
| PGP | Es un programa que da aislamiento al correo electrónico, hace esto cifrando su correo de modo que únicamente la persona prevista pueda leerlo, también es absolutamente capaz de resistir incluso las formas más sofisticadas de análisis dirigidas leyendo el texto cifrado. |
| RETINA | Es un producto de seguridad para red que explora, monitorea, y dispone alarmas, y fija automáticamente vulnerabilidades de la seguridad de la red. |
| SAINT | Es la herramienta integrada de red para el administrador de seguridad, recopila tanta información sobre los ordenadores principal remotos y las redes como sea posible examinando los servicios de red tales como "finger", el NFS, el NIS, el FTP y el REXD y otros servicios. |
| SATAN | (the Security Administrator Tool for Analyzing Networks) es una herramienta de prueba que recolecta una variedad de información acerca de Host de red y fue considerada una de las mejores en su |

| | |
|---|---|
| | momento. Fue diseñado para ayudar a los administradores de sistemas a automatizar el proceso de prueba de sus sistemas frente a vulnerabilidades conocidas que pueden ser explotadas por la red. SATAN esta escrito mayoritariamente en PERL y utiliza un navegador Web como Netscape, Mosaic o Lynx. |
| SNIFFER | Es un analizador robusto del protocolo de red o "succionador" de paquetes, su función es escuchar básicamente el tráfico de la red y produce el análisis basado en el tráfico y/o traduce los paquetes a un cierto nivel de la forma legible humana. |
| SNORT | Es un paquete basado Sniffer/logger que se puede utilizar como sistema ligero para la detección de intrusión en la red. |
| StoneGate | Combina seguridad y continuidad en una sola plataforma, soluciones de Firewall, VPN e IPS, análisis y detección de intrusión, gestión centralizada, escalabilidad y continuidad, con la tecnología multilink, que le permite conectar StoneGate a diferentes ISPs y seleccionar el ISP de menor tiempo de respuesta, asegurando la conectividad y rapidez. |
| TOOLS NMAP | Es un utilitario para las redes grandes de la exploración, control y verificación de puertos. |
| ZoneAlarm | Su categoría es optimizar la configuración por defecto y de manera automática. |

## 4.6 VERIFICACIÓN DEL CONTROL INTERNO

El siguiente programa es un resumen (listado de verificación) de las actividades propuestas en MASTI, en ese sentido se pretende medir el control interno de los sistemas tecnológicos de información a la brevedad posible, debido a que es un formato que recolecta una respuesta cerrada (SI/NO) por parte del auditado, al cual se le demanda honestidad en las respuestas, el consolidado de ambas respuestas le daría una opinión de juicio y análisis al auditor y en este contexto podría tener una idea previa de las fortalezas y debilidades de TI:

| **INSTITUCIÓN:** | **FECHA FIN:** |
|---|---|
| **AUDITOR:** | **FIRMA:** |

| **Áreas / Actividades** | **Número de Referencia** |
|---|---|

**PUNTOS DE CONTROL INTERNO**

Evaluar cuáles son los mecanismos que dispone la alta administración para velar por la estabilidad y la eficiencia de la empresa, en relación a: los sistemas, los equipos, la seguridad, la utilización y los controles aplicados al Área de Tecnología de Información. Verificar con el área responsable de informática el conocimiento y disposición de los siguientes elementos:

**1. Documentación**

| | | |
|---|---|---|
| 1.1 | Organigrama | Si ☐ No ☐ |
| 1.2 | Manual de Puestos | Si ☐ No ☐ |
| 1.3 | Inventario de aplicativos puestos en producción | Si ☐ No ☐ |
| 1.4 | Inventario de programas con su respectiva descripción | Si ☐ No ☐ |
| 1.5 | Inventario de archivos con su respectiva descripción | Si ☐ No ☐ |
| 1.6 | Inventario de hardware | Si ☐ No ☐ |
| 1.7 | Inventario de software | Si ☐ No ☐ |
| 1.8 | Diccionario de Datos | Si ☐ No ☐ |
| 1.9 | Diagramas de Red | Si ☐ No ☐ |
| 1.10 | Diagramas de relación | Si ☐ No ☐ |
| 1.11 | Evaluación de sistemas por parte de auditoría externa | Si ☐ No ☐ |
| 1.12 | Evaluación de sistemas por parte de auditoría interna | Si ☐ No ☐ |
| 1.13 | Plan estratégico | Si ☐ No ☐ |
| 1.14 | Plan de capacitación para el personal | Si ☐ No ☐ |
| 1.15 | Presupuesto anual | Si ☐ No ☐ |
| 1.16 | Políticas y normas que regulen la administración de TI | Si ☐ No ☐ |
| 1.17 | Políticas de Seguridad | Si ☐ No ☐ |
| 1.18 | Políticas de calidad de datos | Si ☐ No ☐ |
| 1.19 | Políticas de Mantenimiento del software | Si ☐ No ☐ |
| 1.20 | Contrato de mantenimiento del hardware | Si ☐ No ☐ |
| 1.21 | Políticas de respaldo | Si ☐ No ☐ |
| 1.22 | Estudios de Factibilidad de los proyectos | Si ☐ No ☐ |
| 1.23 | Plan de trabajo (período actual) | Si ☐ No ☐ |

**2. Servicios con Terceros**

| | | |
|---|---|---|
| 2.1 | Existe contrato de servicios | Si ☐ No ☐ |
| 2.2 | Existe dentro del contrato cláusula de confidencialidad | Si ☐ No ☐ |
| 2.3 | El proveedor ha dado cumplimiento a lo pactado | Si ☐ No ☐ |
| 2.4 | Existen controles para el servicio | Si ☐ No ☐ |

| **INSTITUCIÓN:** | **FECHA FIN:** | |
|---|---|---|
| **AUDITOR:** | **FIRMA:** | |
| **Áreas / Actividades** | | **Número de Referencia** |
| **3. Seguridad** | | |
| 3.1 Control de acceso al personal a la sala de cómputo | Si ☐ No ☐ | |
| 3.2 Identifican, autentican y autorizan el acceso a la Base de Datos | Si ☐ No ☐ | |
| 3.3 Pared de fuego (Firewall) | Si ☐ No ☐ | |
| 3.4 Restringen el tráfico hacia dentro y fuera de la red | Si ☐ No ☐ | |
| 3.5 Software para prevenir, detectar y corregir virus | Si ☐ No ☐ | |
| 3.6 Regulan el correo electrónico | Si ☐ No ☐ | |
| 3.7 Evaluación técnica de infraestructura del edificio | Si ☐ No ☐ | |
| 3.8 Control en las condiciones ambientales | Si ☐ No ☐ | |
| 3.9 Control en los ambientes de desarrollo y producción | Si ☐ No ☐ | |
| 3.10 Controles para la medición de calidad de datos | Si ☐ No ☐ | |
| 3.11 Software para monitorear / analizador redes | Si ☐ No ☐ | |
| 3.12 Herramientas para administrar la seguridad de las Bases de Datos | Si ☐ No ☐ | |
| 3.13 Existen censores ( fuego, humo, movimiento) | Si ☐ No ☐ | |
| **4. Redes** | | |
| 4.1 Evalúan la capacidad y desempeño del hardware. | Si ☐ No ☐ | |
| 4.2 Evalúan la capacidad de la red. | Si ☐ No ☐ | |
| 4.3 Evalúan al proveedor de servicio de comunicaciones. | Si ☐ No ☐ | |
| 4.4 Evalúan la calidad de las operaciones en Internet. | Si ☐ No ☐ | |
| 4.5 Evalúan periódicamente los equipos de comunicación | Si ☐ No ☐ | |

## 4.7 PLAN DE IMPLEMENTACIÓN

El plan de implementación estará sujeto a las instrucciones de la evaluación dadas por la Alta Administración, así como el objetivo y alcance a desarrollar, por ello el auditor de sistemas debe considerar antes de realizar la evaluación los siguientes elementos para su aplicación: planeación, factores de entorno, supervisión, solicitud de requerimientos, programas de auditoría, papeles de trabajo, memorando e informe y el seguimiento.

### 4.7.1 PLANEACIÓN

Las auditorías deberán planearse adecuadamente para asegurarse que se cumplan sus objetivos, y que las revisiones se efectúen conforme a la normatividad aplicable, con la debida oportunidad, eficiencia y eficacia que le corresponde.

Planear la auditoría implica determinar y plasmar en un cronograma de trabajo algunas variables, tales como: aplicativo, rubro por auditar, alcance, objetivos de la revisión, naturaleza, extensión, procedimientos, personal que debe intervenir en el trabajo y el tiempo estimado para cubrir o realizar cada fase de la auditoría. Este cronograma de trabajo deberá revisarse durante la auditoría y en caso necesario, deberá ser ajustado.

El auditor deberá planear su trabajo de modo que la auditoría sea desarrollada de una manera efectiva. Planeación significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperado de la auditoría. La planeación adecuada del trabajo de auditoría ayuda a asegurar que se presta atención a las áreas importantes de la auditoría, y que los problemas potenciales son identificados y que el trabajo es completado en forma oportuna. La planeación también ayuda a la apropiada asignación de trabajo a los auxiliares y para la coordinación del trabajo realizado por otros auditores y técnicos, el tiempo asignado para el desarrollo de la auditoría estará basado en el alcance y objetivos previstos por la administración.

El grado de detalle de planeación variará de acuerdo con el tamaño de la entidad, la complejidad de la auditoría y la experiencia del auditor con la entidad y conocimiento de la actividad del cliente.

Adquirir conocimiento de la actividad del cliente es una parte importante de la planeación del trabajo. El auditor puede desear discutir elementos del plan global de auditoría y algunos procedimientos de auditoría con el comité de auditoría,

administración y personal de la entidad, para mejorar la efectividad, por ello debe de tener en cuenta los siguientes puntos de control:

a. Reconocer el origen de la auditoría
b. Establecer el objetivo de la auditoría
c. Definir el alcance.
d. Determinar las áreas a evaluar
e. Elaborar un cronograma en tiempo versus actividades
f. Elaborar presupuesto según el caso
g. Asignar recursos tecnológicos.
h. Definir el uso de herramientas de auditoría.

### 4.7.2 RECONOCIMIENTO DE FACTORES DEL ENTORNO

El auditor deberá desarrollar y documentar el alcance y conducción esperados según el caso a evaluar, por lo que tendrá que considerar:

a. Factores económicos generales y condiciones de la industria que afectan la empresa.
b. El nivel general de competencia de la administración.
c. Experiencia previa con la entidad y su industria.
d. Evaluación del informe de auditoría anterior.
e. Discusión con personal de auditoría interna y/o externa.
f. Discusión con otros auditores y con asesores legales o de otro tipo que hayan proporcionado servicios a la entidad.
g. Legislación y reglamentos que afecten en forma importante a la Organización.
h. Los términos del trabajo y cualquier responsabilidad estatutaria.

### 4.7.3 SUPERVISIÓN

La auditoría deberá supervisarse en cada una de sus fases y en todos los niveles del personal para garantizar el cumplimiento de sus objetivos.

El responsable de la supervisión deberá ser cuidadoso y tener siempre presente que en los trabajos de auditoría se deben aplicar las normas de auditoría y que la opinión que se vaya a emitir esté justificada y debidamente sustentada por el trabajo realizado.

La supervisión es esencial para asegurarse de que se cumplan los objetivos de la auditoría y el trabajo se ejecute con la calidad necesaria.

### 4.7.4 SOLICITUD DE REQUERIMIENTOS

El auditor debe considerar e identificar algunos requerimientos que le permitirán realizar la auditoría, estos requerimientos deberán ser enviados de forma escrita a la persona responsable o de enlace en la empresa, de forma anticipada estableciendo un plazo de tiempo para la entrega, estos deberán ser proporcionados por el auditado en medios electrónicos o en medios impresos, según el caso, por ejemplo: manual de organización, políticas de seguridad, plan de contingencia, manuales de usuario, diccionario de datos, diagramas de relación, archivos de datos, listado de usuarios, etc.

### 4.7.5 PROGRAMAS DE AUDITORÍA

El auditor deberá aplicar, mejorar y documentar los programas de auditoría propuestos en MASTI, así mismo definirá la naturaleza, oportunidad y alcance de los procedimientos de auditoría planeados que se requieren para implementar la evaluación. El programa de auditoría sirve como un conjunto de instrucciones a los auditores involucrados en la auditoría y como un medio para el control y registro de la ejecución apropiada del trabajo. El programa de auditoría puede también contener los objetivos de la auditoría para cada área y un estimado de horas hombre a invertir en las diversas áreas o procedimientos de auditoría a desarrollar.

Al preparar y modificar el programa de auditoría, el auditor debería considerar las evaluaciones específicas de los riesgos inherentes y de control y el nivel requerido de certeza que tendrán que proporcionar los procedimientos sustantivos. La

coordinación de cualquier ayuda esperada de la entidad, la disponibilidad de los auxiliares y la inclusión de otros auditores o expertos.
Al conocer el alcance del trabajo, queda a juicio del auditor aplicar la totalidad o parcialidad de las actividades definidas en cada área de control de MASTI.

### 4.7.6 PAPELES DE TRABAJO

Los papeles de trabajo son el conjunto de documentos que contienen la información obtenida por el auditor en su revisión, así como los resultados de los procedimientos y pruebas de auditoría aplicados; con ellos se sustentan las observaciones, recomendaciones, opiniones y conclusiones contenidas en el informe correspondiente. Todos los resultados y recomendaciones de la auditoría deberán sustentarse con evidencia obtenida en la auditoría, deberá documentarse debidamente en los papeles de trabajo, principalmente con el objeto de: Contar con una fuente de información y en su caso, efectuar aclaraciones con el ente auditado u otras partes interesadas y dejar constancia del trabajo realizado para futura consulta y referencia. Los auditores deberán considerar que el contenido y disposición de sus papeles de trabajo reflejarán el grado de su competencia y experiencia, estos deberán ser completos y detallados que pueda servirse de ellos para conocer el trabajo en que se sustente el informe de auditoría.

En conclusión la evidencia debe ser suficiente y apropiada en la auditoría para poder extraer conclusiones razonables sobre las cuales basa su informe, en ese contexto la **evidencia en la auditoría:** Significa la información obtenida por el auditor para llegar a las conclusiones, asimismo comprenderá documentos fuentes, la evidencia en la auditoría se obtiene de una mezcla apropiada de pruebas de control, de procedimientos sustantivos, análisis de proyecciones y análisis de indicadores y las **pruebas de control**: Significa pruebas realizadas para obtener evidencia en la auditoría sobre lo adecuado del diseño y operación efectiva de los sistemas, control interno, el cumplimiento de las metas y objetivos propuestos y el grado de eficacia, economía y eficiencia y el manejo de la entidad.

Para obtener las conclusiones de la auditoría, el auditor normalmente examina toda la información disponible, con base a los siguientes factores:

a. Nivel del riesgo.
b. Naturaleza de los sistemas y el control interno.
c. Evaluación del riesgo de control.
d. Experiencia obtenida en auditorías previas
e. Resultados de procedimientos de auditoría, incluyendo fraude o error que puedan haberse encontrado.
f. Fuente y confiabilidad de información disponible.

Por tanto, los papeles de trabajo estarán bajo la custodia de Auditoría de Sistemas ó de la instancia a la que pertenece, por contener la evidencia de trabajos de auditoría realizados por su personal.

La confidencialidad está ligada al cuidado y diligencia profesional con que deberán proceder los auditores, el uso y consulta de los papeles de trabajo estarán vedados por el secreto profesional a personas ajenas al área, salvo requerimiento o mandato de la autoridad jerárquica o legal de su competencia.

### 4.7.6.1 OBTENCIÓN PARA LA EVIDENCIA EN LA AUDITORÍA

El auditor de sistemas obtiene evidencia en la auditoría por uno o más de los siguientes procedimientos:

a. La inspección consiste en examinar registros, documentos, o activos tangibles. La inspección de registros y documentos proporciona evidencia en la auditoría de grados variables de confiabilidad dependiendo de su naturaleza y fuente y de la efectividad de los controles internos sobre su procesamiento.

b. La observación consiste en mirar un proceso o procedimiento que está siendo realizado por otros, incluye toma fotográfica.

c. La revisión consiste en buscar la información adecuada, dentro o fuera de la Organización, estas podrán variar dependiendo la información a recolectar.

d. La entrevista consiste en la respuesta a una pregunta o solicitud para corroborar la información obtenida en la investigación.

e. Los procedimientos analíticos consisten en el análisis de índices, indicadores y tendencias significativas incluyendo la investigación resultante de fluctuaciones y relaciones que son inconsistentes con otra información relevante.

### 4.7.6.2 FORMA Y CONTENIDO DE LOS PAPELES DE TRABAJO

El auditor deberá preparar papeles de trabajo que sean suficientemente completos y detallados para proporcionar una comprensión global de la auditoría.

La extensión de los papeles de trabajo es un caso de juicio profesional, ya que dependiendo la naturaleza de la Organización y el alcance determinarán el volumen o profundidad de los papeles, estos a su vez podrán ser:

a. Información referente a la estructura organizacional de la entidad.
b. Extractos o copias de documentos legales importantes, convenios u otro texto.
c. Resumen de las principales leyes, reglamentos y normas que debe cumplir la entidad.
d. Información concerniente a la industria, entorno económico y entorno legislativo dentro de los que opera la entidad.
e. Evidencia del proceso de planeación incluyendo programas de auditoría y cualesquier cambio al respecto.
f. Evidencia de las pruebas realizadas en el control interno.
g. Evidencia de evaluaciones de los riesgos inherentes y de control y cualesquiera revisiones al respecto.

h. Evidencia de la consideración del auditor del trabajo de auditoría interna y las conclusiones alcanzadas.
i. Análisis de transacciones.
j. Análisis de tendencias, índices importantes e indicadores económicos.
k. Una indicación sobre quién desarrolló los procedimientos de auditoría y cuándo fueron desarrollados
l. Copias de documentación sobre comunicaciones con otros auditores, expertos y terceras partes.

### 4.7.6.3 MARCAS PARA LOS PAPELES DE TRABAJO

La finalidad principal de las marcas en los papeles de trabajo es para identificarlos mejor, su utilidad radica en que tienen un significado preciso ya que destacan aspectos importantes de los papeles de trabajo que ha medida se van revisando, con el uso de estos símbolos se evita el abuso en la recopilación de copias inútiles de papeles de evaluación, por otra parte las referencias en los papeles de trabajo tienen la finalidad de facilitar y de relacionar la observación con el informe.

## 4.7.7 EL MEMORANDO (INFORME PRELIMINAR)

No es una práctica recomendable, aunque sí usual en algunos casos, ya que el Informe de Auditoría es por principio, un informe de conjunto. Sin embargo, en el caso de detección de irregularidades significativas, tanto errores como fraudes, sobre todo se requiere una actuación inmediata según la normativa legal y profesional, independientemente del nivel jerárquico afectado dentro de la estructura.

La finalidad principal del memorando, informe preliminar o borrador de informe no es formal sino que es representación de comunicar al auditado de manera inmediata las observaciones identificadas, con base en los resultados que se vayan obteniendo en el proceso de la auditoría, es decir que son avances sobre las observaciones para corrección, queda a criterio del auditor también poderlas enviar vía correo electrónico o impreso, todo esto es con el objetivo de dejar en el informe final aquellas que no fueron posible corregirlas durante el proceso de evaluación, con relación a las

observaciones que fueron superadas, estas se documentan y se señalan en el informe.

### 4.7.8 EL INFORME FINAL

Una vez que se ha detectado los hallazgos u observaciones, es obligación del auditor comentarlas de forma directa y abierta con los responsables asignados, a fin de que conozcan, acepten, aclaren, complementen y/o las modifiquen con detalles y pruebas.

Un informe final con su dictamen u opinión sobre los resultados, deberán ser superados por las áreas involucradas de la Organización, en el tiempo según la importancia y exigencia de cada observación.

El informe de auditoría de sistemas puede definirse como un documento formal y oficial que utiliza el auditor para informar por escrito y de manera oportuna, precisa, completa, sencilla y clara, sobre los resultados que obtuvo después de haber aplicado las técnicas, métodos y procedimientos apropiados al tipo de revisión que realizó, para fundamentar con ellos su opinión respecto a la auditoría realizada y estar en condiciones de poder emitir un dictamen correcto sobre el comportamiento de la tecnología de información. El informe de auditoría debe contener, como mínimo las siguientes secciones:

#### 4.7.8.1 CARTA EJECUTIVA (OFICIO DE PRESENTACIÓN)

Es la primera parte del informe de auditoría y es un documento de carácter oficial que sirve como presentación consolidada del informe, mediante al cual se le expone a la Alta Administración de la empresa o a la jefatura correspondiente a quien reporte el auditor, un resumen general de los hallazgos. Esta carta contiene los siguientes aspectos: (anexo F modelo de carta ejecutiva)

a. Logotipo de identificación.

   Se trata de poner el logotipo, emblema o símbolo que permita identificar a la empresa o al área al cual pertenece auditoría de sistemas.(no es mandatario)

b. Nombre de la empresa.

Si la evaluación la realizó una entidad externa se coloca el nombre de la empresa, caso contrario se coloca el nombre del área al cual depende auditoría de sistemas.

c. Ubicación física y fecha de emisión de la carta

Esto identifica el lugar y la fecha que se emite la carta ejecutiva.

d. Identificación del área o empresa auditada

Se coloca el área, departamento, sistema al cual fue evaluado.

e. Nombre del personal receptor de la carta ejecutiva.

Por lo general, este informe se remite a un ejecutivo de alto nivel de la empresa o al jefe a quién reporta el auditor de sistemas (los grados académicos son reglas de cortesía)

f. Período de evaluación.

En esta parte se anotan las fechas de inicio y finalización de la auditoría; con esto se busca darle a conocer al receptor del informe el tiempo que comprendió la evaluación.

g. Contenido.

Es una breve descripción de los puntos que fueron evaluados y de los aspectos que integran el informe, su redacción debe ser precisa, esquemática y clara.

h. Responsable de emitir el dictamen.

En esta parte se anota el nombre del profesional responsable de emitir la carta ejecutiva, o el nombre del auditor de sistemas, según políticas internas de cada institución.

i. Firma.

En esta parte se pone la firma autógrafa del responsable de la auditoría, que es la persona que adquiere el compromiso de avalar lo reportado.

### 4.7.8.2 PRESENTACIÓN DEL INFORME.

Se consideran al inicio los mismos literales de la carta ejecutiva “a,b,c,d,e” este permite de una forma más amplia las observaciones identificadas en la evaluación, así mismo está formada por los siguientes elementos: ( anexo G modelo de Informe)

a. Breve introducción al Informe.

En esta parte se anotan las razones que dieron origen a la auditoría, quién la ordenó, área o sistemas a revisar, actividades sujetas a evaluación, estos elementos permiten fundamentar las razones del porqué se realizó la auditoría.

b. Contenido del informe.

Se hace una breve descripción de los puntos que fueron evaluados, describiendo en forma clara, los aspectos que se consideran como observaciones o desviaciones sobre los puntos de los programas de auditoría.

c. Listado de observaciones.

Se describen las observaciones o situaciones que necesitan mejorarse; queda a criterio del auditor presentarlas de importancia mayor a importancia menor, cabe señalar que cada observación se encuentra relacionada o referenciada a un papel de trabajo.

d. Recomendaciones.

Después de haber señalado la observación, el auditor puede recomendar de manera objetiva, libre de cualquier influencia y con estricto apego a las pruebas y resultados observados durante la evaluación.

e. Responsable.

Se deja el nombre, puesto y titulo del responsable de emitir el informe, además de su firma autógrafa.

### 4.7.9 SEGUIMIENTO

Consiste en realizar un monitoreo o seguimiento a las observaciones señaladas en el informe con la finalidad de identificar el estado de estas, las cuales pueden llegar a ser: superadas, no superadas, en proceso o no aplica al proceso actual. Independientemente del estado que presenten las observaciones, estas deben ser evaluadas por el auditor de sistemas con la finalidad de fortalecer el área tecnológica. Con relación al tiempo de iniciar el seguimiento queda a juicio del auditor o jefatura a la cual reporta.

### 4.7.10 FECHA DEL INFORME

El período de realización del examen puede ser flexible, la fecha del Informe es importante, no sólo por la cuantificación de honorarios y el cumplimiento con el cliente, sino para conocer la magnitud del trabajo y sus implicaciones. Conviene precisar las fechas de inicio y conclusión del trabajo de campo, como períodos probables para la toma de decisiones. No obstante algunas ocasiones la fecha de finalización puede verse afectada debido a los hallazgos y al grado de riesgo identificado, al respecto, será decisión de la Alta Administración la ampliación ó reducción del tiempo estipulado.

## 4.8 COMPOSICIÓN DE MASTI

El Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información, conocido como "MASTI", agrupa las siguientes divisiones:

**Planificación y Organización:**
Comprende las decisiones estratégicas y planes operativos definidos por la Administración, esto incluye el entorno organizacional, elementos que contribuirán al logro de los objetivos planeados por la Entidad.

**Plataforma Tecnológica:**
La práctica de las estrategias definidas por la Organización, obligan a la directriz responsable de TI a cumplir bajo soluciones integrales y tecnológicas, proporcionar un mejor servicio ante el crecimiento y demanda que la institución requiere, todo ello con la finalidad de hacer posible la continuidad de las operaciones, descargando su confianza en los sistemas informáticos.

**Soporte:**
El mantenimiento, control y seguridad son factores a considerar como complemento de los procesos de TI debido a que deben ser evaluados regularmente, tanto en calidad como cumplimiento, ya que es parte fundamental para la continuidad del servicio.

**Subcontratación.**
Un acuerdo de subcontratación es aquel que se establece entre una entidad y un proveedor de servicios, en el que este último realiza una actividad, función, proceso o administra los recursos de TI del negocio solicitante. Las razones para que una empresa requiera de subcontratación están en función del alcance, naturaleza, ubicación, proveedor, calidad, recursos, oportunidad, servicios, etc.

## 4.9. APLICACIÓN DE MASTI

Los programas de auditoría podrían llegar a aparentar la facilidad de su aplicación, sin embargo, podemos decir que no es una actividad plenamente mecánica sino que es necesario tener conocimientos y la capacidad de medir el alcance debido a que esta es una actividad de análisis crítico, la cual no implica que existan fallas en la entidad auditada sino más bien fortalecer y mejorar el servicio de TI.

El Marco Referencial de MASTI "Manual de Auditoría de Sistemas para la Evaluación de la Tecnología de Información", proporciona al auditor de sistemas una herramienta que le permite guiarlo sobre los puntos importantes a evaluar dentro de la Organización, no obstante la experiencia de éste, podrá hacer la ampliación o reducción del mismo, estando sujeto a la responsabilidad y la objetividad que defina los lineamientos de la Administración de la cual depende.

En nuestra opinión tenemos la certeza que los recursos de TI deben ser segmentados en divisiones, y éstas compuestas en áreas más específicas. Como producto de ello presentamos cuatro principales divisiones en las que se sustenta el presente manual: Planificación y Organización, Plataforma Tecnológica, Soporte y Subcontratación. Las divisiones en referencia se agrupan en **30** áreas de control y estas a la vez se subdividen en **541** actividades seccionadas las cuales conforman los programas de auditoría. La numeración correlativa de las actividades descritas en los referidos programas no representan, ni obedecen un orden de importancia, más bien es un numero correlativo, asimismo las actividades en comento no son obligatorias en su totalidad para la aplicación de cada una de estas, debido a que son de carácter general, de forma que permita la aplicación en cualquier tipo de organización, este enfoque resultó como producto de las pruebas realizadas del trabajo de aplicación en el campo.

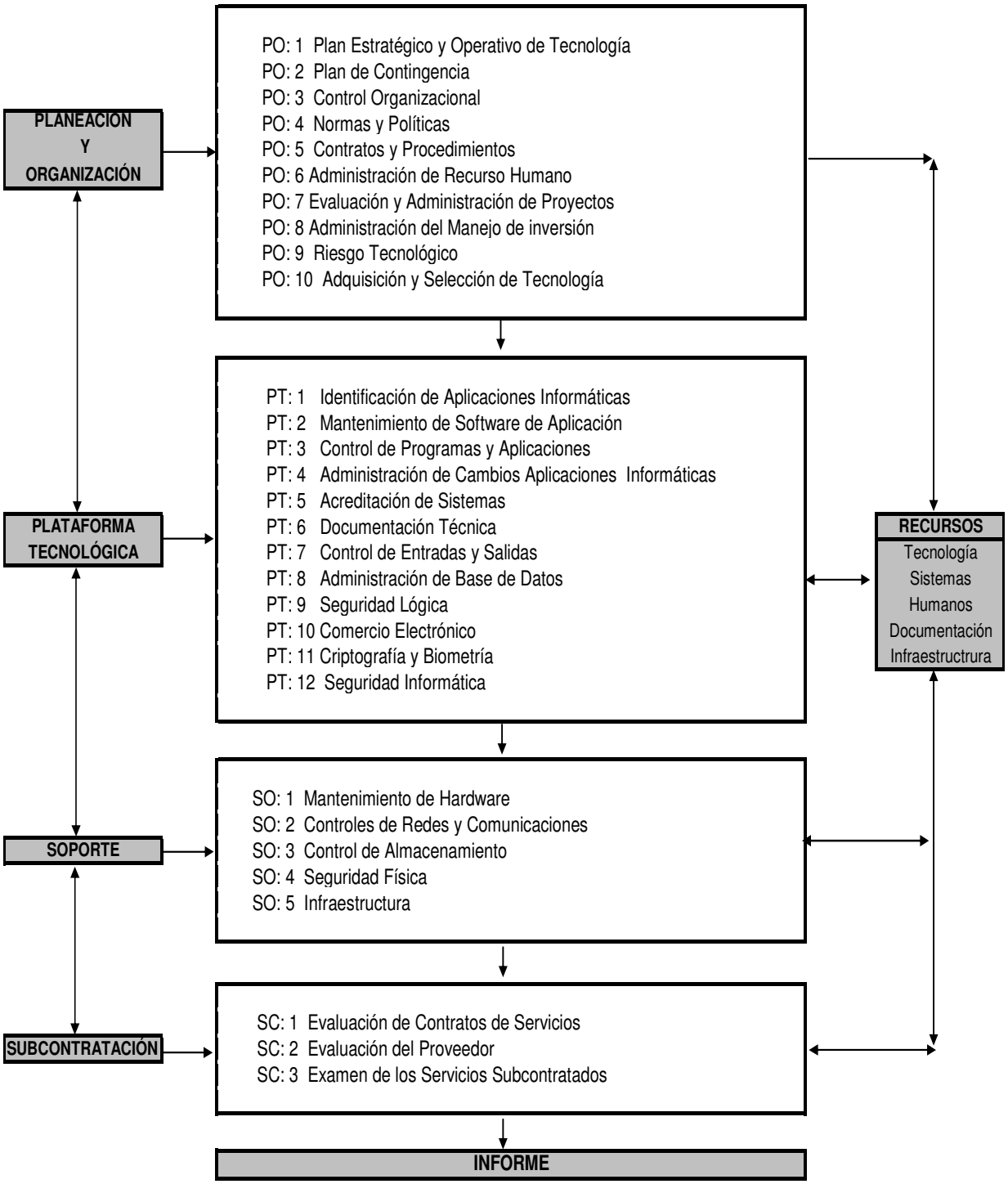
Los programas de auditoría descritos en MASTI, se encuentran orientados a objetivos de control en TI, que permitirán a la Administración tener una evaluación de carácter técnico sobre el ambiente de TI en la Organización y los riesgos asociados a esta actividad y los resultados obtenidos que permita mejorar el

servicio tecnológico en: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, todo ello encaminado a que la tecnología apoye el logro de los objetivos estratégicos institucionales.

## 4.10 ESQUEMA DE MASTI

El siguiente esquema representa el proceso que indica al auditor de sistemas, el flujo interactivo que pueden efectuar al realizar la evaluación, donde se observa que las cuatro divisiones están ligadas y se retroalimentan o se complementan con las actividades que dependen de cada una de ellas, el proceso en referencia estará bajo el juicio y el conocimiento que el auditor quiera profundizar en el alcance y objetivo previsto, esto requerirá la necesidad de disponer o involucrar para el desarrollo algunos recursos tales como: tecnológicos, de sistemas, recursos humanos, documentación técnica operativa y administrativa e infraestructura tecnológica.

**ESQUEMA DE FLUJO PARA LA APLICACIÓN DE MASTI**



## 4.11 MANUAL DE AUDITORÍA DE SISTEMAS PARA LA EVALUACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN. (MASTI)

**(Ver Manual de Auditoría)**

**ÁREAS** Páginas

# MANUAL DE AUDITORÍA DE SISTEMAS PARA LA EVALUACIÓN DE LA TECNOLOGÍA DE INFORMACIÓN.

# (MASTI)

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PLANEACION Y ORGANIZACIÓN ( PO)** | |
| **PO1: PLAN ESTRATÉGICO Y OPERATIVO DE TECNOLOGÍA.** | |
| 1. Verificar si en el plan estratégico institucional se encuentra incluido el plan estratégico de TI. | |
| 2. Verificar si las actividades y metas del plan estratégico de TI están alineados, con los objetivos estratégicos institucionales y dar seguimiento al cumplimiento de los proyectos a largo plazo. | |
| 3. Verificar la existencia de un plan operativo de TI para dar seguimiento al cumplimiento de metas de los proyectos a corto plazo. | |
| 4. Verificar las actividades, períodos, grado de avance y responsables de ejecución de las actividades del plan estratégico. | |
| 5. Verificar que el plan estratégico de TI sea traducido periódicamente en planes a corto plazo. | |
| 6. Verificar si la Alta Administración o Auditoría Interna realiza monitoreo sobre el desarrollo e implementación de los Planes de TI a Corto y Largo Plazo, para contribuir al cumplimiento de los objetivos y metas de dichos planes. | |
| 7. Verificar si en el proceso de planificación se han considerado factores internos y externos que afectan a la institución y su entorno por ejemplo: la distribución geográfica, la evolución tecnológica, los costos administrativos y operativos, los requerimientos legales, las regulaciones y leyes que rigen el funcionamiento de la Entidad. | |
| 8. Evaluar si la institución tiene los recursos tecnológicos y humanos suficientes para el desarrollo del proyecto bajo las condiciones establecidas inicialmente. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 9. Verificar los insumos o fuentes de información que se utilizarán como base para la elaboración de la planeación estratégica de TI. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO2: PLAN DE CONTINGENCIA**<br><br>1. Identificar la existencia del plan de contingencia y obtener una copia, así mismo verificar la fecha de vigencia, última actualización y funcionario responsable de autorización.<br><br>2. Verificar que el plan hace referencia a normas y políticas dictadas por tecnología.<br><br>3. Verificar si el plan está orientado a superar procesos críticos e imprevistos en el menor tiempo posible.<br><br>4. Verificar si la estructura y lenguaje del documento general es entendible y comprensible para su aplicación.<br><br>5. Verificar que en el plan se encuentren definidas las tareas a realizar para cada una de las personas involucradas en el plan.<br><br>6. Verificar que en el plan se hayan considerado pruebas para distintos escenarios y los mecanismos para la solución, por ejemplo: fallas en servidores centrales, fallas en servidores de servicio, fallas en el suministro eléctrico, fallas en los enlaces de comunicación, falta de insumos, respaldos no actualizados, etc.<br><br>7. Verificar que las jefaturas dispongan de una copia actualizada del plan.<br><br>8. Identificar si el plan incluye o describe la participación de un comité de administración de desastres o del equipo de emergencia.<br><br>9. Verificar si existe un servidor de contingencia para todas las aplicaciones críticas.<br><br>10. Verificar que el plan disponga de un anexo con los nombres del personal de soporte, administrativo y proveedores de servicio, el cargo, número telefónico fijo y móvil. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 11. Realizar llamadas telefónicas a parte del personal involucrado en el plan con la finalidad de verificar que los números son correctos y están actualizados.<br><br>12. Verificar que el plan se haya probado al menos dos veces al año, con la finalidad de fortalecer las áreas no funcionales.<br><br>13. Entrevistar al personal para identificar si conocen las responsabilidades que tienen asignadas en una situación de desastre.<br><br>14. Verificar si existen procedimientos definidos para actualizar el manual. Asimismo si aplican y distribuyen las actualizaciones a los usuarios involucrados.<br><br>15. Verificar que el plan contenga los planos del centro de cómputo, diagramas de cableado eléctrico, diagramas de red, diagramas de ductos e inventarios de hardware.<br><br>16. Verificar que exista una copia de datos actualizados, programas y documentación técnica del sistema que almacene en un lugar externo a la empresa.<br><br>17. Verificar que el personal involucrado tiene el conocimiento de los procedimientos establecidos para la continuidad de las operaciones en caso de desastres.<br><br>18. Evaluar si el centro de cómputo alterno o para la continuidad de operaciones reúne las condiciones mínimas de seguridad física tales como: controles de acceso, piso elevado o protegido, controles de humedad, controles de temperatura, circuitos especializados, fuente interrumpida de energía, dispositivos de detección de agua, detectores de humo y un sistema adecuado de extinción de incendios. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO3: CONTROL ORGANIZACIONAL**<br><br>1. Solicitar el organigrama de la empresa e identificar la ubicación de TI, analizar su estructura jerárquica y que esté conforme a la situación actual. Así mismo verificar su vigencia y aprobación.<br><br>2. Verificar si la estructura actual está encaminada a los logros de los objetivos del área de TI.<br><br>3. Verificar si los niveles jerárquicos establecidos actualmente son necesarios y suficientes para el desarrollo de las actividades del área de TI.<br><br>4. Verificar si se consideran adecuados los departamentos y áreas en que está dividida la estructura de TI.<br><br>5. Solicitar los manuales de puestos del área de TI y verificar que las funciones descritas correspondan con las que ejecuta cada empleado de TI.<br><br>6. Evaluar el manual de puestos, su claridad en la delegación de autoridades, y que deben ir acompañadas de definiciones de las habilidades técnicas necesarias, para utilizarse como base para la evaluación del desempeño.<br><br>7. Verificar si los puestos actuales son adecuados a la necesidad que tiene el área para cumplir con sus funciones.<br><br>8. Verificar que mecanismo utiliza la administración para resolver los conflictos por las cargas de trabajo desequilibradas.<br><br>9. Identificar las causas de incumplimiento de las funciones y objetivos previstos por la Administración, como por ejemplo: falta de personal, personal no capacitado, cargas de trabajo excesivas, realización de otras actividades, planificación y la forma en que se desarrollan. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar que la posición de la unidad de tecnología esté en un nivel suficientemente alto para garantizar su independencia de los departamentos usuarios.<br><br>11. Verificar si en los manuales de reclutamiento de personal, consideran la educación, la experiencia y los riesgos de trabajo pertinentes para los requerimientos del puesto y del grado de responsabilidad.<br><br>12. Verificar que exista una separación adecuada de tareas entre los operadores de la computadora, los programadores de la Aplicación y los analistas de sistemas.<br><br>13. Verificar que existan controles externos apropiados de manera que el personal administrativo, operativo y técnico esté informado e involucrado en las actividades ya definidas.<br><br>14. Asegurar una adecuada separación de deberes entre la preparación manual de los datos y las funciones de transferencia de los datos a la computadora, grabación manual en cinta o disco magnético, etc.<br><br>15. Verificar que exista un plan de capacitación y que éste responda a las necesidades de la institución en cumplimiento al plan estratégico de TI.<br><br>16. Verificar que todo el personal tome un mínimo de cinco días consecutivos de vacaciones, de manera que alguien mas pueda ejecutar las funciones específicas de un puesto determinado.<br><br>17. Verificar que exista una política o norma apropiada para la separación de funciones y esta sea auditada.<br><br>18. Revisar las descripciones de los puestos por cada departamento o unidad, de tal manera asegurar que cada una de ellas está conforme al cargo. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO4: NORMAS Y POLÍTICAS**<br><br>1. Solicitar inventario de políticas y normas establecidas para TI.<br><br>2. Verificar que la Administración o la Gerencia de TI sea responsable de la formulación, desarrollo, documentación, divulgación y el control de las políticas; y que todas ellas estén por escrito y debidamente autorizadas y actualizadas.<br><br>3. Verificar que la Gerencia de TI haya creado mecanismos de divulgación que permitan asegurar que las políticas sean comunicadas y comprendidas por todo el personal involucrado directa o indirecta con el área de TI.<br><br>4. Verificar que las políticas o normas emitidas sean actualizadas, por lo menos anualmente o al momento de presentarse cambios significativos en el ambiente operacional, para garantizar que sean funcionales y aplicables.<br><br>5. Verificar si las políticas o normas son del conocimiento y aceptadas por el personal de TI.<br><br>6. Verificar la existencia de política o normas sobre reserva y confidencialidad de información.<br><br>7. Verificar que las normas y políticas estén autorizadas por la alta administración y que presenten fecha de vigencia.<br><br>8. Verificar que exista una participación de las áreas especializadas de la institución en la creación y regulación de las normas y políticas. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO5: CONTRATOS Y PROCEDIMIENTOS ADMINISTRATIVOS.**<br><br>1. Verificar que los procedimientos de trabajo ejecutados por los operadores del centro de cómputo estén documentados por escrito.<br><br>2. Verificar que los procedimientos escritos definan los horarios de trabajo para los operadores del centro de cómputo, considerando los cierres semanales, mensuales y anuales.<br><br>3. Verificar si existe un control para restringir el acceso al personal externo a TI en días y horarios de procesos especiales.<br><br>4. Verificar que exista un control manual o automático de la información que entra y sale del área TI.<br><br>5. Verificar si existe un responsable oficial encargado de la oficina de control de la información para toda la organización, teniendo como una de sus funciones principales ser el enlace de la información entre TI y el resto de la organización.<br><br>6. Verificar la existencia de procedimientos a utilizar por los operadores del centro de cómputo, de forma que permitan identificar el inicio, proceso y final de cada actividad.<br><br>7. Verificar la existencia de una póliza de seguro con cobertura para la pérdida de equipo de computación y medios de proceso de datos.<br><br>8. Solicitar las hojas de vida de los principales puestos de TI para evaluar la capacidad y experiencia para desarrollar su puesto. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO6. ADMINISTRACIÓN DEL RECURSO HUMANO.**<br><br>1. Verificar que se considera en el proceso de selección de personal el nivel educativo, y la experiencia laboral en el puesto para el cual está participando.<br><br>2. Verificar si existe evaluación del personal para garantizar un nivel aceptable de desempeño y cumplimiento de metas del área de TI.<br><br>3. Verificar si existe un plan de capacitación y si está orientado al giro de la institución y la plataforma tecnológica con que cuenta la institución.<br><br>4. Verificar si la Gerencia de TI ha considerado pruebas de entrenamiento cruzado, con la finalidad de disponer con personal de respaldo ante posible ausencia de personal clave.<br><br>5. Verificar que la Gerencia de TI considere acciones oportunas y apropiadas con respecto a cambios de puestos y despidos.<br><br>6. Verificar que exista la suficiente formación del personal, con capacitación continua que ayude a mantener su conocimiento técnico, sus destrezas y habilidades.<br><br>7. Verificar si el desempeño de los empleados se evalúa contra los estándares establecidos.<br><br>8. Verificar si los puestos actuales son adecuados a la necesidad que tiene el área para llevar a cabo sus funciones.<br><br>9. Verificar si el número de empleados que trabajan actualmente en el área de TI es adecuado para cumplir con las funciones encomendadas.<br><br>10. Verificar si las cargas de trabajo están distribuidas de forma equitativa para todo el personal de TI. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 11. Verificar si son adecuadas las condiciones ambientales con respecto a: espacio, iluminación, ventilación, equipo de oficina, mobiliario, ruido, etc. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO7: EVALUACIÓN Y ADMINISTRACIÓN DE PROYECTOS.**<br><br>1. Verificar si existe un comité técnico evaluador de proyectos e identificar los miembros que la integran; asimismo verificar si existe un libro de actas de los acuerdos y decisiones tomadas sobre los proyectos.<br><br>2. Verificar si existe documentación histórica sobre la ejecución de los proyectos finalizados o en proceso.<br><br>3. Verificar la existencia de cumplimientos de las normas internas para la formulación de proyectos.<br><br>4. Verificar si la institución cuenta con controles para evaluar periódicamente la ejecución del proyecto, de forma que permita evaluar la situación actual y efectuar las medidas correctivas necesarias, como cambios en el entorno del negocio y en la tecnología, para lograr la finalización del proyecto cumpliendo con las metas y objetivos requeridos.<br><br>5. Verificar que la Gerencia de TI haya establecido una metodología de Administración de Proyectos que defina como mínimo, la asignación de responsabilidades, el detalle completo de las tareas, el cronograma de trabajo, los recursos, los diversos puntos de revisión y los procedimientos para las aprobaciones.<br><br>6. Verificar que para los proyectos de TI considerados importantes para la institución exista un estudio de factibilidad tecnológica de cada alternativa de forma que satisfaga los requerimientos de la institución.<br><br>7. Verificar que para los proyectos de TI importantes para la institución exista un estudio costo beneficio de cada alternativa de forma que cubra los requerimientos de la institución. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 8. Verificar de la planeación de los proyectos de TI y comprobar la existencia de lo siguiente:<br><br>8.1 Verificar si existe un acta de inicio y autorización de la alta administración.<br>8.2 Verificar que estén definidos los miembros y responsables del equipo del Proyecto.<br>8.3 Verificar si poseen plan de aseguramiento de calidad de sistemas.<br>8.4 Verificar si posee un Plan de Pruebas (piloto, paralelo, modular, etc.)<br>8.5 Verificar si el plan considera contrataciones de personal adicional para el proyecto<br>8.6 Verificar si cuentan con un Plan de capacitación.<br>8.7 Verificar si cuentan con un plan de pruebas de estrés para las aplicaciones informáticas.<br>8.8 Verificar que exista un plan de Revisión Post Implementación<br>8.9 Verificar que la documentación de las aplicaciones informáticas se lleve actualizada.<br>8.10 Verificar que exista una programación financiera del proyecto.<br><br>9. Verificar que el área de TI tenga documentado la planeación de los proyectos finalizados, en proceso y los que estén por iniciar.<br><br>10. Verificar la plataforma tecnológica a utilizar para el desarrollo de los proyectos de TI, esto incluye base de datos, sistema operativo, software de desarrollo, etc.<br><br>11. Verificar que exista un comité de evaluación de proyectos con la responsabilidad de emitir actas que documenten los avances del proyecto y las decisiones tomadas en dicho comité.<br><br>12. Verificar que la Gerencia de tecnología tenga claramente definido las ventajas de la nueva tecnología a implantar y los riesgos asociados a cada una de ellas. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO8: ADMINISTRACIÓN DEL MANEJO DE INVERSIÓN.**<br>1. Verificar la existencia de un presupuesto operativo anual para adquisición de tecnología.<br>2. Verificar que la compra de equipos y software estén de conformidad al presupuesto asignado para tal efecto.<br>3. Verificar que el presupuesto contemple cantidades realistas y coherentes con los precios de mercado de la tecnología de información y que cumplan con los planes estratégicos y operativos.<br>4. Verificar las licitaciones o matriz técnica de ofertas y analizar según proveedor y condiciones del producto.<br>5. Verificar que los cambios en el presupuesto anual y anterior estén de conformidad a las variaciones en los precios de mercado y necesidades de la institución. Cualquier variación considerable, pedir la justificación respectiva al personal que ha desarrollado dicho presupuesto.<br>6. Verificar que exista un control adecuado de los costos en que incurre el área de Tecnología de Información.<br>7. Verificar que existan procedimientos y políticas claras, definidas y documentadas respecto al monitoreo de costos.<br>8. Verificar que los excesos en comparación al presupuesto, sean controlados, justificados y se les de el seguimiento correspondiente, para cumplir con la proyección anual realizada<br>9. Verificar que los costos en que incurra la institución sean claramente justificados.<br>10. Verificar que toda salida de efectivo vaya acompaña de más de una firma, a fin de que quede reflejado quien realizó el desembolso, quien lo revisó y quien lo autorizó. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| | |
| **PO9: RIESGO TÉCNOLOGICO**<br><br>1. Verificar si existen normas o políticas para la Administración del Riesgo Tecnológico.<br><br>2. Verificar si existe un comité de evaluación de riesgo tecnológico.<br><br>3. Verificar si el comité tiene definido como identifica y mide el riesgo tecnológico.<br><br>4. Verificar si el aspecto de confidencialidad mantiene controles estrictos y si se han adoptado medidas de seguridad, sobre todo con las transferencias de datos que viajan a través de Internet, donde cabe la posibilidad que se coloquen "Sniffers" a la puerta de un servidor donde se realicen operaciones monetarias ó intercambios de documentos con información confidencial.<br><br>5. Verificar los procedimientos y mecanismos optados por TI para la identificación y autenticación de usuarios en la red, para garantizar la legitimidad de las operaciones que estos realizaron.<br><br>6. Verificar la existencia de procedimientos, prácticas y políticas de control interno, y si estos son adecuados.<br><br>7. Verificar si la institución ha incurrido en pérdidas derivadas de fraudes o errores; y establezca lo adecuado de las medidas adoptadas por la administración para minimizar este riesgo.<br><br>8. Verificar el nivel de competencia y capacidad de los funcionarios que hacen efectivo los procedimientos de control interno.<br><br>9. Verificar la idoneidad, experiencia y capacidad técnica del personal que realiza el trabajo de auditoría externa de sistemas. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar el nivel o grado de independencia de auditoría externa de sistemas tomando en consideración las recomendaciones que realiza a la Administración.<br><br>11. Verificar la efectividad de las actividades de auditoría externa de sistemas con relación a: objetivos, alcance, frecuencia, documentación apropiada, conclusiones, anexos, etc.<br><br>12. Verificar si el sistema de Información Gerencial provee al usuario información oportuna y de calidad, consistente, completa y relevante para la toma de decisiones, principalmente aquellas enfocadas a la administración de riesgos.<br><br>13. Verificar lo adecuado de la organización, lugar, recursos y la idoneidad del personal del área de sistemas de información, en función de la labor desempeñada, responsabilidad e independencia dentro de la organización.<br><br>14. Verificar la existencia y aplicación de medidas apropiadas que le den seguridad a la infraestructura y limiten el acceso a los recursos tecnológicos, así como a la información generada por dichos sistemas y su adecuado almacenamiento.<br><br>15. Verificar el cumplimiento en lo relacionado al uso de subcontratación o actividades de consultores externos, la existencia de políticas y procedimientos adecuados y alineados a la protección y no divulgación de la información.<br><br>16. Verificar si la institución cuenta con una adecuada planificación a corto y largo plazo para el cambio de infraestructura tecnológica y para los sistemas de información conforme a las tendencias del mercado y el mismo crecimiento de la institución.<br><br>**17. Riesgo operacional o transaccional.**<br>17.1 Verificar qué mecanismos utilizan para medir la confiabilidad e integridad de los sistemas de información. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 17.2 Verificar la seguridad en las transacciones enviadas o recibidas.<br>17.3 Verificar si han recibido ataques internos o externos a los sistemas informáticos.<br><br>18. Verificar el cumplimiento de beneficios propuestos, tales como:<br>18.1 Rapidez y agilidad en las transacciones.<br>18.2 Tiempo de respuesta razonable.<br>18.3 Costos de transacción más bajos.<br>18.4 Accesos a nuevos mercados<br>18.5 Seguridad.<br>18.6 Menos gastos fijos y de operación.<br>18.7 Servicio sin restricción de tiempo.<br>18.8 Acceso desde cualquier parte.<br>18.9 Mejor imagen.<br><br>19. **Riesgo Dependencia Tecnológica**.<br>19.1 Verificar si en el contrato de adquisición de software no existe cláusula que obligue a la empresa a disponer exclusivamente del producto por tiempo definido.<br>19.2 Verificar que el software sea de arquitectura abierta, con el fin de poder migrar a una nueva plataforma.<br>19.3 Verificar los períodos de vigencia de uso de los módulos, para determinar el grado de obsolescencia.<br>19.4 Verificar la disposición de los proveedores al realizar el cambio de plataforma.<br>19.5 Verificar el estatus del proveedor del software y determinar si en la actualidad de representante o distribuidor.<br>19.6 Verificar cuando el servicio informático es subcontratado, existe disposición de acceso a los datos.<br><br>20. **Riesgo Legal.**<br>20.1 Verificar si existen litigios pendientes de ser resueltos, asociados a tecnología.<br>20.2 Verificar si el tratamiento que se da al riesgo legal en los nuevos productos a lanzar al mercado y la protección de la institución en la elaboración de contratos es adecuada. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 20.3 Verificar la frecuencia y el nivel de gravedad de los litigios a nivel tecnológico que se ha visto involucrada la institución, y evalúe su historial.<br>20.4 Verificar si el contrato sobre las pólizas de seguro, ha sido revisado por el asesor legal de la institución y las opiniones que ha vertido sobre el mismo.<br>20.5 Verificar que la institución cumpla con la normativa legal y reglamentaria, establecidas en las leyes de la República de El Salvador.<br><br>**21. Riesgo de Reputación**<br><br>21.1 Verificar con la Administración la disposición de políticas, prácticas y procedimientos respecto del manejo de la imagen o reputación de la empresa.<br><br>21.2 Verificar si monitorean el comportamiento de funcionarios y empleados que se relacionen con las licitaciones y compras de equipo tecnológico.<br><br>21.3 Verificar como la Administración evalúa la percepción del público, respecto del servicio, estabilidad y calidad.<br><br>21.4 Verificar el volumen de reclamos del público, respecto a fraudes realizados por medio de sistemas informáticos, así como las medidas adoptadas para subsanar las deficiencias. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PO:10 ADQUISICIÓN Y SELECCIÓN DE TECNOLOGÍA**<br><br>1. Verifique el cumplimiento de normas internas para la compra de tecnología.<br><br>2. Verifique el estudio inicial sobre la necesidad del requerimiento, según el monto de la inversión.<br><br>3. Verificar si el comité técnico evalúa cada inversión a realizar en tecnología.<br><br>4. Verificar cuál es el criterio de evaluación en adquisición de software y hardware.<br><br>5. Verificar si revisan los documentos fiscales correspondientes al hardware y software contratados, con la finalidad de comprobar los desembolsos.<br><br>6. Verificar si comparten con el personal responsable del área de informática las condiciones contractuales brindadas por el proveedor.<br><br>7. Verificar como se evalúa la nueva adquisición de hardware y software, conforme al condicionamiento del sistema actual.<br><br>8. Verificar si existe planificación en la migración de los datos con el proveedor y se definen responsabilidades internas dentro de la Organización.<br><br>9. Verificar que criterios técnicos usan para seleccionar al proveedor.<br><br>10. Verificar como se realiza la adquisición de equipo se realiza a través de licitación para los proveedores.<br><br>11. Verificar como analizan las fortalezas y debilidades de los proveedores versus características, por medio de una matriz técnica. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 12. Verifique si el estudio de viabilidad reúne las condiciones de la factibilidad técnica, operativa y financiera.<br><br>13. Verificar que procedimientos utilizan para la aplicación y desglose del porcentaje en cada desembolso.<br><br>14. Verificar la consideración en la adquisición de hardware o software la relevancia del proveedor de ser representante o distribuidor.<br><br>15. Verificar como evalúan la experiencia de otras organizaciones en cuanto al uso del producto.<br><br>16. Verifique en el universo de sus clientes la calidad del servicio proporcionado por el proveedor. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PLATAFORMA TECNOLÓGICA (PT)**<br><br>**PT1: IDENTIFICACIÓN DE APLICACIONES INFORMÁTICAS.**<br><br>1. Verificar si existe un inventario de software aplicativo en el que se detalle la versión, el proveedor, la vigencia de la licencia, etc.<br><br>2. Verificar el inventario de software contra las licencias, con el objetivo de evitar sanciones por la Ley de propiedad intelectual.<br><br>3. Verificar si el software es sensitivo cuando es utilizado en lugares remotos, considere el hacer una carga especial del software desde el lugar central. Este daría la seguridad de que no se hayan hecho cambios ilegales en los programas en lugar remoto. También verificar si se puede cargar así los programas cada vez que un proveedor de mantenimiento lo requiera.<br><br>4. Verificar que el software de seguridad controle las tablas sensitivas y que valide periódicamente contra acceso no autorizado el cambio de la configuración original.<br><br>5. Verificar que no se permita a los programadores de las aplicaciones modificar y ejecutar directamente programas en ambiente de producción.<br><br>6. Verificar que mecanismos se utilizan para prevenir probables intrusiones tipo “caballo de Troya”, es decir que el usuario carga al sistema un programa de software autorizado que contiene programa ó rutinas no autorizadas.<br><br>7. Verificar que existan controles sobre los recursos compartidos en los equipos informáticos como: discos duros, carpetas o archivos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT2: MANTENIMIENTO DE SOFTWARE DE APLICACIÓN.**<br><br>1. Verificar si el diseño de las nuevas aplicaciones o de las modificaciones a los módulos puestos en producción, son revisados y aprobados por la Gerencia de TI.<br><br>2. Verificar e Identificar quienes son los responsables de aprobar cualquier proyecto de desarrollo, implementación o modificación.<br><br>3. Verificar si existen procedimientos definidos o estándares, para las etapas de desarrollo de un nuevo sistema o cambios a los ya existentes.<br><br>4. Verificar si cuentan con mecanismos para identificar los requerimientos de seguridad y control interno para cada proyecto de desarrollo o modificación de sistemas de información, previo a su desarrollo.<br><br>5. Verificar e identificar si se incluyen en el diseño de las nuevas aplicaciones o en las modificaciones de sistemas de información, controles de aplicación que garanticen que los datos de entrada y salida estén completos.<br><br>6. Verificar si consideran aspectos básicos de seguridad y control interno del módulo a ser desarrollado o modificado, y estos son evaluados junto con el diseño conceptual del mismo.<br><br>7. Identificar si existe una metodología estándar para el desarrollo de un plan de pruebas, en donde se incluyan pruebas unitarias, pruebas de aplicación, pruebas de integración y pruebas de carga y estrés, para cada módulo.<br><br>8. Verificar si la formulación del procedimiento de prueba y los datos de prueba son revisados y aprobados por el jefe de programación. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 9. Verificar si se aplican adecuadas medidas de seguridad para prevenir divulgación de información sensitiva durante las pruebas.<br><br>10. Verificar que los resultados de las pruebas son revisados y aprobados por el usuario. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT3: CONTROLES DE PROGRAMAS Y APLICACIONES.**<br><br>1. Verificar el conteo de la cantidad de "byte" de los programas fuentes actuales para hacer una comparación rápida entre la cantidad de byte de estos y los autorizados que se trasladaron a producción para alertar en caso de modificaciones.<br><br>2. Verificar que exista un archivo lóg o bitácora que permita identificar los errores de ejecución de aplicaciones, sistema operativo y BD.<br><br>3. Verificar si han considerado todos los dispositivos de seguridad que fueron recomendados por el fabricante o el programador.<br><br>4. Verificar que exista una persona responsable en el área de TI de revisar periódicamente los archivos lóg o bitácoras de los sistemas.<br><br>5. Verificar que la institución respete los límites de la capacidad de procesamiento recomendados por el proveedor como: memoria, espacio en disco, procesamiento CPU. Para garantizar el correcto funcionamiento de las aplicaciones informáticas.<br><br>6. Verificar que la institución cuente con un servidor de desarrollo que sea de uso de los programadores para el desarrollo y pruebas de las aplicaciones internas.<br><br>7. Verificar que los programadores no tengan acceso a la línea de comandos, en los servidores de producción y acceso a estos para consultas.<br><br>8. Verificar si existe una persona responsable dentro del área de tecnología en cargada de ejecutar programas de diagnóstico de la red institucional.<br><br>9. Verificar que exista un procedimiento de control de cambios de los programas y del traslado del ambiente de desarrollo a producción. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar que no exista más de un usuario además del administrador con el perfil de mantenimiento de parámetros de los módulos de las aplicaciones informáticas.<br><br>11. Comprobar que la custodia de la documentación del software de Aplicación, los software utilitario entre otros estén controlados por personal de tecnología. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT4: ADMINISTRACIÓN DE CAMBIOS DE APLICACIONES INFORMÁTICAS.**<br><br>1. Verificar si existe un sistema para el control de requerimientos de usuarios que afecten la estructura de los sistemas de información.<br><br>2. Verificar el o los tipos de formularios utilizados para el control de cambios<br><br>3. Verificar si existen procedimientos definidos para determinar el estatus de cada solicitud para los cambios realizados.<br><br>4. Verificar el procedimiento para el tratamiento de solicitudes identificadas como urgentes.<br><br>5. Verificar la existencia de controles para la modificación de programas fuentes y el traslado a producción.<br><br>6. Verificar si se mantiene un registro de cambios en los programas, que indique la fecha en que se realizó, a fin de proveer el orden cronológico exacto del sistema. Asimismo identificar el responsable de realizar el cambio.<br><br>7. Verificar si se requiere de la aprobación y autorización por escrito de la Gerencia de TI, para todas las modificaciones antes de hacer cambios.<br><br>8. Verificar si los cambios al sistema operacional o programas aplicativos, sus pruebas y resultados, son revisados por el jefe de programación técnica o quien hace sus funciones.<br><br>9. Verificar si los usuarios que formularon el requerimiento lo revisan y dan su aprobación a dichos cambios. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar si existen disposiciones para probar los cambios de programas y revisar los resultados con personal de supervisión antes de que dichas revisiones sean trasladadas al ambiente de producción.<br><br>11. Verificar quienes son los encargados de efectuar los cambios y como se documentan.<br><br>12. Verificar que las pruebas se realizan en un área o servidor de desarrollo. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT5: ACREDITACIÓN DE SISTEMAS.**<br><br>1. Verificar si como parte de cada proyecto de desarrollo, implementación o modificación de sistemas de información, existe un procedimiento para que los elementos necesarios del sistema anterior sean convertidos al sistema nuevo.<br><br>2. Verificar si se planifica la migración de los datos con el proveedor y se definen responsabilidades.<br><br>3. Verificar que existan certificaciones independientes en que la conversión del sistema y datos se desarrolle de acuerdo al plan establecido.<br><br>4. Verificar si las pruebas a los nuevos sistemas o a las modificaciones a los sistemas, son llevadas a cabo por un grupo de prueba independiente, diferente al de los desarrolladores.<br><br>5. Verificar que las pruebas a los sistemas se desarrollen en un ambiente de prueba separado, el cual sea representativo del ambiente operacional futuro (por ejemplo: condiciones similares de seguridad, controles internos, cargas de trabajo, etc.)<br><br>6. Verificar si cuentan con procedimientos establecidos para asegurar que las pruebas piloto o en paralelo sean llevadas a cabo con planes pre establecidos.<br><br>7. Verificar si los criterios para la terminación del proceso de prueba son especificados con anterioridad.<br><br>8. Verificar si incluyen como parte del plan de instalación y acreditación de sistemas, pruebas de aceptación por parte de los usuarios finales de los sistemas nuevos o de las modificaciones a los sistemas de información. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 9. Verificar como certifican los usuarios finales la aceptación final del nuevo sistema o de las modificaciones a los sistemas.<br><br>10. Verificar el procedimiento utilizado para asegurar que la Gerencia usuaria acepta formalmente el nivel de seguridad para los sistemas.<br><br>11. Verificar el proceso utilizado para el traslado de nuevas aplicaciones o modificaciones al sistema a producción.<br><br>12. Verificar quién es el responsable de efectuar el traslado a producción. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT6: DOCUMENTACIÓN TECNICA**<br><br>1. Verificar por medio de inventario los nombres de programas y descripción de ellos<br><br>2. Verificar por medio de Inventario los nombres de tablas o archivos con su respectiva descripción<br><br>3. Verificar la existencia y disponibilidad de diagramas de entidad relación.<br><br>4. Verificar la existencia de manuales de usuario de los aplicativos puestos en producción.<br><br>5. Verificar si los manuales de usuarios se encuentran autorizados y disponen de fecha de vigencia, con la finalidad de identificar su actualización<br><br>6. Verificar la existencia de diccionario de datos de las tablas o archivos que conforman los sistemas puestos en producción. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT7: CONTROL DE ENTRADAS Y SALIDAS**<br><br>**ENTRADAS (ORIGEN DE TRANSACCIONES)**<br><br>1. Verificar según sistema cuáles y cuántos son los aplicativos que se alimentan de forma automática y manual.<br><br>2. Verificar si la estructura de los formularios que se utilizan como base para la captura de información son adecuados y completos de acuerdo a lo requerido por el sistema.<br><br>3. Verificar la existencia de aplicativos que se alimentan por medio de dispositivos magnéticos de entidades externas, asimismo comprobar los mecanismos de control de calidad de los datos.<br><br>4. Verificar e identificar filtros de alertas o mensajes del sistema que permitan controlar la calidad de información que será ingresada.<br><br>5. Verificar según muestra de documentos fuente, aspectos como cifras de control firma de autorización y similares.<br><br>6. Verificar si existe un control a nivel de perfil de usuarios que ingresan datos para evitar ingreso de datos por usuarios no autorizados.<br><br>7. Verificar que existan restricciones controladas para el uso de diversos dispositivos magnéticos de entrada.<br><br>8. Verificar que cuando se diseñen formas, los campos de datos importantes tengan predefinido un formato de ingreso de datos, con el fin de minimizar errores.<br><br>9. Verificar que existan controles sobre los documentos de propiedad con números de series secuenciales y el ingreso de dichos números al sistema para crear la relación entre ambos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar que exista un registro de la fecha de proceso y la fecha de transacción para las transacciones de entrada.<br><br>11. Verificar si a los documentos ingresados, se les asigna una marca de control o sello con la finalidad de asegurase que estos no sean ingresados nuevamente.<br><br>12. Verificar qué mecanismos utilizan para identificar si existen documentos de entrada no ingresados al sistema.<br><br>13. Verificar el cumplimiento del artículo de 451 y 455 del Código de Comercio, que relaciona al período de resguardo de la información fuente u original.<br><br>14. Comprobar el control utilizado para demostrar que la información a ingresar se encuentra autorizada.<br><br>15. Identificar si la institución realiza un control de calidad sobre el estado de los documentos que van a ser digitalizados para ser almacenados como imagen.<br><br>16. Verificar qué procedimientos existen para el manejo de errores con el fin de proporcionar al personal usuario instrucciones para la corrección de errores en los documentos fuentes.<br><br>17. Revisar los tipos de errores y las razones de su ocurrencia con el fin de determinar si los problemas son ocasionados por el programa o por ingreso incorrecto de datos.<br><br>18. Verificar si se obtiene una copia del LOG que registra el sistema en relación a las entradas de datos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SALIDAS**<br><br>1. Verificar si existe un inventario de reportes, que identifique: nombre del programa, nombre del módulo, unidad destino, frecuencia de emisión y medio de emisión.<br><br>2. Verificar el proceso de distribución de los reportes de manera que se envíen al personal autorizado.<br><br>3. Verificar el área donde se resguardan los reportes confidenciales de manera que el personal no autorizado no pueda tener acceso a ellos.<br><br>4. Comprobar que se eliminen de forma inmediata los archivos de salida, no finalizados cuando sean confidenciales.<br><br>5. Verificar que exista un responsable de efectuar un análisis general de los reportes con el objeto de determinar si hay reportes que puedan ser eliminados, fusionados, reagrupados, simplificados, o si se requiere nuevos reportes.<br><br>6. Evaluar quién ejerce la función de control de calidad en los reportes emitidos.<br><br>7. Verificar si los encabezados de cada reporte incluyen los siguientes aspectos: fecha de generación, nombre del programa, período cubierto de proceso, titulo descriptivo del contenido del reporte, usuario que generó, número de identificación del programa, número de página, etc.<br><br>8. Verificar que se etiquete cada reporte o grupo de reportes de manera que se indique en el nombre del usuario, destino y el área o departamento al que pertenece.<br><br>9. Verificar la existencia de códigos que identifiquen el nivel de confidencialidad del reporte. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar cuál es el procedimiento para la destrucción de reportes sobrantes o que no estén en uso.<br><br>11. Verificar que mecanismos de control utilizan para producir únicamente la cantidad requerida de reportes solicitados.<br><br>12. Evaluar el nivel de satisfacción de los usuarios respecto a la estructura de los reportes y a la confidencialidad de la información generada. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT8: ADMINISTRACIÓN DE BASE DE DATOS.**<br><br>1. Verificar qué mecanismos o herramientas usa el Administrador de Base de Datos (DBA) para supervisar y administrar la Base de Datos.<br><br>2. Verificar el procedimiento utilizado para definir el nivel de acceso de los usuarios.<br><br>3. Verificar si únicamente el Administrador de Base de Datos tiene privilegios a nivel de administrador para hacer cambios a la base de datos.<br><br>4. Verificar los diferentes tipos de usuarios que tienen acceso a la Base de Datos, e identificar su clasificación por medio de la siguiente segmentación:<br>4.1 Usuarios que modifican la estructura<br>4.2 Usuarios que modifican los datos<br>4.3 Usuarios operativos<br>4.4 Usuarios técnicos<br><br>5. Verificar que el Administrador de Base de Datos disponga de procedimientos escritos para la restauración de la Base de Datos, en caso de una destrucción total o parcial.<br><br>6. Verificar que el usuario y clave del BDA se registre en un sobre lacrado y éste se resguarde en un lugar seguro.<br><br>7. Verificar que el Administrador de Base de Datos sea responsable de la integridad de la Base de Datos y desarrolle reglas de validación y acceso.<br><br>8. Verificar que el Administrador de Base de Datos documente cualquier cambio que se realice a la Base de Datos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 9. Verificar que el Administrador de Base de Datos administra el diccionario de datos.<br><br>10. Verificar que el Administrador de Base de Datos es el responsable de la seguridad global de la Base de Datos.<br><br>11. Verificar si el Administrador de Base de Datos tiene control para que no se realicen pruebas en la Base de Datos en producción, sino que se disponga de diferentes ambientes para este fin.<br><br>12. Verificar que los usuarios no tengan acceso directo a la Base de Datos, sino que el acceso sea a través del servidor de aplicaciones.<br><br>13. Verificar si existen pruebas que involucren atentados deliberados para destruir o modificar la Base de Datos, considérense atentados tanto internos como externos. Estos simulacros deben de ser desarrollados por el Administrador de Base de Datos. Las destrucciones descritas en los simulacros deben de ser llevados a cabo por personal autorizado o no autorizado que trate de cambiar la Base de Datos, modificar los programas de la Aplicación, sustraer copia de la Base de Datos o del diccionario de datos, etc.<br><br>14. Verificar que solo el usuario de administrador tenga el privilegio de acceso a las tablas de usuarios y contraseñas.<br><br>15. Verificar si el software de Base de Datos utilizado en la institución cuenta con tablas de registros de auditoría para revisar los eventos que tiene registrados.<br><br>16. Verificar en las tablas de registros de auditoría de la Base de Datos las acciones de intentos de conexión, acceso a los objetos y accesos a la base. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 17. Verificar las acciones que el Administrador de la Base de Datos realiza con las tablas de registros de auditoría de la base, para corregir posibles fallas o accesos no autorizados.<br><br>18. Verificar que el parámetro para permitir auditoría a la Base de Datos tenga el valor que equivale o permite auditoría.<br><br>19. Verificar que existan controles mínimos en la seguridad de las tablas: por ejemplo:<br><br>19.1 Clase de transacción: un usuario específico puede quedar limitado a ciertos tipos de transacciones.<br>19.2 Programas: los usuarios pueden estar restringidos al empleo de ciertos programas de proceso.<br>19.3 Grupos de archivos: se les puede permitir a los usuarios el acceso, la modificación, y el borrado únicamente de archivos específicos.<br>19.4 Archivos completos: puede ser dado el acceso a un conjunto completo de archivos.<br>19.5 Registros individuales: el acceso puede estar limitado a registros específicos.<br>19.6 Grupos de registros: a usuarios específicos se les puede permitir o restringir el uso de determinados grupos de registro.<br>19.7 Diversos controles de contraseña: los usuarios pueden quedar limitados al uso de solo ciertas porciones de la Base de Datos.<br>19.8 Diversos controles de terminales: varias terminales pueden quedar sujetas a un código de transacciones para restringir su acceso a ciertas porciones de la base de datos.<br>19.9 Controles del circuito: ciertos circuitos en la red de comunicación de datos pueden quedar limitados a ciertas porciones de la base de datos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT9: SEGURIDAD LÓGICA.**<br><br>1. Verificar que el software de comunicaciones exige código de usuario y contraseña para su acceso.<br><br>2. Verificar si los usuarios no pueden acceder a ningún sistema, sin antes haberse autenticado correctamente en la red institucional.<br><br>3. Verificar si se inhabilita al usuario después de ingresar la contraseña después un número determinado de intentos fallidos.<br><br>4. Verificar que el sistema operativo obliga a cambiar la contraseña periódicamente.<br><br>5. Verificar que la contraseña no sea menor a 8 caracteres y que sea una combinación de números y letras, entre ellos mayúsculas y minúsculas.<br><br>6. Verificar que las contraseñas no son mostradas en pantalla cuando se ingresan.<br><br>7. Verificar si durante el procedimiento de identificación, los usuarios son informados de cuándo fue su última conexión para ayudar a identificar potenciales suplantaciones o accesos no autorizados.<br><br>8. Verificar que existe software para llevar estadísticas que incluyan tasas de errores y de retransmisión.<br><br>9. Verificar que los equipos puedan validar la identificación electrónica de las terminales que se agregan a la red. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT10: COMERCIO ELÉCTRONICO**<br><br>1. Verificar que la organización disponga de documentación relacionada al e_commerce, tales como :<br>1.1 Planificación del proyecto al menos contendrá: objetivos y alcances, estudio de viabilidad, costo beneficio y plataforma tecnológica.<br>1.2 Copia de contratos de lo proveedores de servicio.<br>1.3 Copias de contratos del mantenimiento de equipo.<br>1.4 Descripción y esquema de la plataforma tecnológica.<br>1.5 Política de configuración.<br>1.6 Esquemas de red<br>1.7 Esquema de seguridad lógica.<br>1.8 Diagramas de entidad relación.<br>1.9 Diccionario de datos.<br>1.10 Inventario de aplicativos puestos en producción<br>1.11 Manual de Usuario de los aplicativos puestos en producción.<br>1.12 Pruebas de vulnerabilidad.<br>1.13 Estrategias del negocio y la necesidad de operaciones electrónicas.<br><br>**2. Controles**<br><br>2.1 Verificar el volumen de información y los servicios utilizados<br>2.2 Verificar quienes tienen acceso a los diagramas de configuración del sistema.<br>2.3 Verificar los distintos reportes emitidos por el sistema.<br>2.4 Verificar el reporte de caídas del sistema, medir la frecuencia y magnitud de las mismas.<br>2.5 Verificar en las transacciones de pago las medidas de seguridad implementadas y que estas incluyan autenticación de usuarios, consistencia de datos y confidencialidad de las operaciones<br>2.6 Verificar quienes son los responsables de la seguridad de las operaciones electrónicas.<br>2.7 Hacer pruebas en el sitio para conocer de los productos y los servicios ofrecidos.<br>2.8 Verificar los mecanismos de privacidad asociado a la creación de contraseñas y usuarios del sistema. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 2.9 Verificar si el proceso para la administración de contraseñas de los sistemas de e_commerce, consideran aspectos como caracteres permitidos, cantidad mínima de caracteres, fechas de expiración, número de fallos permitidos y acción frente a las fallas, procesos para cambio de contraseñas entre otros.<br>2.10 Verificar si existe cumplimiento de los servicios ofrecidos en la parte legal y contractual, ofertada y publicada.<br>2.11 Verificar si la Organización tiene un proceso adecuado parar el control de las transacciones.<br>2.12 Verificar si existe un sistema de encripción adecuado para las operaciones realizadas en el sistema.<br>2.13 Verificar si existen mecanismos adecuados para proteger la reserva de los datos personales de sus clientes que utilizan el servicio.<br>2.14 Verificar si las firmas digitales son emitidas, manejadas y/o certificadas por un proveedor externo.<br>2.15 Verificar si existe control en las versiones y procedimientos de distribución de software, para las aplicaciones relacionadas con e_commerce<br>2.16 Verificar las técnicas utilizadas por la Organización para monitorear la seguridad de los sistemas de e_commerce.<br>2.17 Verificar si la Organización cuenta con un software para análisis de seguridad, si es utilizado y cual es su alcance.<br>2.18 Verificar si la administración requiere el uso de firmas digitales para autenticar a los usuarios en relación a las transacciones.<br>2.19 Verificar si disponen de herramientas para monitorear y detectar intromisiones a la red.<br>2.20 Verificar si la opinión de los usuarios que usan los servicios son consideradas en las proyecciones de crecimiento y la planeación de los recursos de la e_commerce.<br><br>**3. Normativas**<br><br>3.1 Verificar si las políticas de seguridad incluyen adecuadamente el tema de encripción y los mecanismos que utilizan. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 3.2 Verificar si las políticas incluyen el uso de software para la detección de virus, y los mecanismos usados para la actualización. | |
| 3.3 Verificar si las políticas de los cortafuegos (Firewalls) definen responsabilidad por su mantenimiento, dominios de acceso y reglas que permitan tráfico permitido y prohibido. | |
| 3.4 Verificar si las políticas de seguridad incluyen lineamientos de control de acceso a la red y a los datos. | |
| 3.5 Verificar la existencia de un proceso para evaluar periódicamente la composición de productos de e_commerce y las necesidades del mercado tecnológico. | |
| 3.6 Verificar si el e_commerce es consistente con la misión del Organización y los planes estratégicos. | |
| **4. Corta fuego (Firewall)** | |
| 4.1 Verificar si la Organización dispone de un proceso adecuado para identificar cualquier acceso remoto, diferente que el Firewall, y como la administración monitorea y controla ese acceso. | |
| 4.2 Verificar la adecuación del proceso para restringir acceso a la documentación de la configuración del Firewall. | |
| 4.3 Verificar el procedimiento utilizado por los responsables de la administración de los Firewall para prevenir el acceso no autorizado a la red interna. | |
| 4.4 Verificar los procesos que la Organización utiliza para controlar el acceso no autorizado a la sala de los Firewall. | |
| 4.5 Verificar los procedimientos usados para la certificación las pruebas y actualización políticas en los cortafuegos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **Prevención de virus.**<br><br>5.1 Verificar el cumplimiento realizado por los usuarios para prevenir los virus informáticos.<br><br>5.2 Verificar si la Organización tiene un proceso adecuado para detectar y prevenir virus asociados a los sistemas de e_commerce.<br><br>5.3 Verificar si existe un proceso adecuado para actualizar el anti virus, y si la revisión de virus en la máquina se realiza periódicamente | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT11: CRIPTOGRAFIA Y BIOMETRIA**<br><br>**Criptografía**<br><br>1. Verificar los elementos protegidos bajo ambiente criptográfico.<br><br>2. Verificar que herramientas utilizan para proteger la información<br><br>3. Verificar si el cifrado es simétrico, es decir utilizar la misma clave para cifrar y descifrar un documento.<br><br>4. Verificar si el cifrado es asimétrico, es decir que es aquella en que el sistema de cifrado usa dos claves diferentes, una es la clave pública y que se puede enviar a cualquier persona y otra que se llama clave privada.<br><br>5. Verificar si el cifrado es híbrido, en donde el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico.<br><br>6. Verificar si el cifrado se realiza bajo ambiente PGP (pretty good privacy), al menos debe disponer de: firma digital, encriptación del mensaje, comprensión y segmentación.<br><br>7. Verificar que para el cifrado existan dentro del servicio de red los Protocolos de comunicación tales como: TLS, SSL, SET, OpenPGP, DSS, SSH.<br><br>8. Verificar que tipo de algoritmo utilizan para el cifrado de datos, por ejemplo: AES, BLOWFISH, CAST-128. CAST-256, DES-X, ROT-13, RSA, Triple DES, Twofish, skipjack, etc.<br><br>9. Verificar la existencia de otros algoritmos tales como Sustitución Mono alfabética ó Poli alfabética , transposición, etc. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar de que procedimientos o herramientas disponen para la autentificación:<br>10.1 Mediante una firma (Firma Digital): la cual debe garantizar la procedencia de un mensaje conocido, de forma de poder asegurar que no es una falsificación.<br>10.2 Mediante una contraseña: la cual debe garantizar la presencia de un usuario autorizado mediante una contraseña secreta y correcta.<br>10.3 Mediante un dispositivo: se debe garantizar la presencia de un dispositivo válido en el sistema, por ejemplo una llave electrónica<br><br>11. Verificar si el certificado digital dispone de los siguientes elementos:<br>11.1 Nombre distintivo de la entidad, incluye la información de identificación (el nombre distintivo) y la llave pública.<br>11.2 Nombre distintivo de la Autoridad Certificadora. Identificación y firma de la Autoridad Certificadora (CA) que firmó el certificado.<br>11.3 Período de validez, tiempo durante el cual el certificado es válido.<br>11.4 Información adicional, puede contener información administrativa de la Autoridad Certificadora (CA) como un número de serie o versión<br><br>12. Verificar qué autoridad certificadora es la que ha sido contratada para el servicio, por ejemplo: VeriSign, Thawte Certificación, Xcert Sentir CA, Emtrust, Cybertrust, etc.<br><br>**Biometría**.<br><br>1. Verificar si disponen de políticas para el uso de biometría.<br><br>2. Verificar quienes son los responsable de la administración del sistema biométrico.<br><br>3. Verificar que método es usado en la organización, por ejemplo: ojo-iris, ojo-retina, huellas dactilares, geometría de la mano, escritura, firma, voz. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 4. Verificar el hardware y software para el servicio y uso de biometría.<br><br>5. Verificar el procedimiento para crear un usuario o eliminarlo del sistema según el método biométrico usado.<br><br>6. Verificar el contrato con el proveedor e identificar fortalezas y debilidades<br><br>7. Verificar la plataforma tecnológica usada e identificar capacidades de almacenamiento y futura expansión. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **PT12: SEGURIDAD INFORMÁTICA**<br><br>1. Verificar que existan políticas de seguridad, definidas y aprobadas por la Administración.<br><br>2. Verificar que las políticas de seguridad contengan, elementos como: confidencialidad, integridad y disponibilidad.<br><br>3. Verificar que las políticas contengan mecanismos para medir: riesgos y amenazas, análisis de riesgos, plan de seguridad, controles preventivos y correctivos, plan de contingencia, biometría, firma digitales, protección y defensas.<br><br>4. Identificar qué mecanismos utilizan para no revelar la información a personas no autorizadas, acceso a información confidencial y protección de datos.<br><br>5. Verificar como controlan las amenazas externas, como hackers o espías.<br><br>6. Verificar la existencia de procedimientos para controlar riesgos como por ejemplo: ausencia de planes de contingencia, ausencia de políticas de seguridad y estrategias, ausencia de procedimientos para modificación de aplicaciones, programadores con acceso irrestricto a los datos, seguridad débil en accesos a Internet, e-mail, Inadecuada segregación de funciones, falta de procedimientos de contingencia, débiles políticas para la creación de contraseñas, ausencia de bitácoras de seguridad y falta de oficiales de seguridad.<br><br>7. Verificar la existencia de procedimientos para controlar las amenazas, por ejemplo: Sniffing, Frame Spoofing, Crack, Hacking a un Website, Ingeniería Social, Caballos de Troya, Ataques de Denegación de servicios, Fake Mail. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 8. Verificar si están definidas las funciones de los cargos siguientes: el DBA (Data base administrator - administrador de base de datos), el NA (Administrador de red - Network administrator) y el SA (Administrador de sistema - System administrator). Dicha verificación es con la finalidad de no entrar en conflicto de funciones.<br><br>9. Verificar que tipo de sistemas de detección de intrusos (IDS) utilizan según las características siguientes:<br><br>9.1 HIDS (*HostIDS*): un IDS vigilando un único ordenador y por tanto su interfaz corre en modo no promiscuo. La ventaja es que la carga de procesado es mucho menor.<br>9.2 NIDS (*NetworkIDS*): un IDS basado en red, detectando ataques a todo el segmento de la red. Su interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.<br>9.3 *DIDS (DistributedIDS*): sistema basado en la arquitectura cliente servidor compuesto por una serie de NIDS (IDS de redes) que actúan como censores centralizando la información de posibles ataques en una unidad central que puede almacenar o recuperar los datos de una base de datos centralizada. La ventaja es que en cada NIDS se puede fijar unas reglas de control especializándose para cada segmento de red. Es la estructura habitual en redes privadas virtuales (VPN)<br><br>10. Verificar como administran los perfiles de los responsables de la seguridad, ó al menos que cumplan con las actividades siguientes:<br>SecAdmin: Administrador de seguridad. Administra altas, bajas, y cambios de perfiles de usuarios. Otorga permisos de acceso a los recursos y puede auditar a los usuarios.<br>System Administrator: Instalación de software de base, administración de recursos (capacidad, performance, etc.). Sin acceso irrestricto a los datos. Con utilización controlada de utilitarios sensitivos.<br>Network Administrator: Atiende y monitorea la red. Instala y configura los componentes de software y hardware. Resuelve problemas de ambiente y conexiones. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: | |
|---|---|---|
| INSTITUCIÓN: | FECHA FIN: | |
| AUDITOR: | FIRMA: | |
| **Áreas / Actividades** | | **Referencia** |

DBA: Administra la base de datos. Genera las estructuras, los índices, el diccionario de datos, administra los espacios, etc.

Desarrollador: Puede modificar programas, compilar en librerías de test, y probar con datos de prueba. EL desarrollador puede tener línea de comandos restringidos.

Implementador: Debe pasar los programas de desarrollo a producción mediante un mecanismo que asegure la transparencia. Puede intervenir operaciones. El implementador puede tener línea de comandos restringidos.

Operador del sistema: Puede operar el sistema, encenderlo, apagarlo, descolgar usuarios por terminales, etc. El operador no debe tener línea de comandos.

Usuarios finales: Solo deben acceder a las aplicaciones mínimas que necesitan para desarrollar su tarea diaria.

11. Verificar que la seguridad informática y de datos, se aborda un proceso de seguridad recomendado a utilizar según las siguientes herramientas: un Firewall o combinación de ellos, Proxy es un sistema de detección de intrusos o IDS. sistemas de actualización automática de software, sistemas de control de la integridad de los servidores, paquetes, etc.

12. Verificar como se administra la información según los lineamientos establecidos en la Política de Seguridad de Información, aprobada por la Alta Dirección.

13. Verificar como establecen y mantienen los procedimientos que aseguren la integridad, confidencialidad, exactitud y disponibilidad de la información de la empresa, en niveles concordantes con la importancia que se merece.

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 14. Verificar los riesgos a que pueda estar expuesta la información, ya sea durante su almacenamiento, manipulación o comunicación, y recomendar los controles más adecuados según criterios de costo/beneficio, para eliminarlos o reducir sus efectos.<br><br>15. Verificar como monitorean y rastrean la actividad de los usuarios administrativos y operativos a fin de detectar y corregir desviaciones en el uso correcto de la información, o en el cumplimiento de las normas y procedimientos asociados a la seguridad de la información.<br><br>16. Verificar que controles lógicos y físicos se utilizan para asegurar que sólo el personal autorizado pueda acceder a la información, dentro de los niveles de atención.<br><br>17. Verificar que procedimientos operativos y programas computarizados idóneos, probados y autorizados, se pueda acceder, modificar, divulgar, destruir o mantener la Información.<br><br>18. Verificar el cumplimiento de las políticas de desarrollo de documentación mínima de los procedimientos operativos y aplicaciones, que permitan las operaciones de la empresa bajo una situación de contingencia.<br><br>19. Evaluar y seleccionar, en coordinación con la unidad de Sistemas tecnológicos, herramientas para apoyar las funciones de la unidad Seguridad de Informática.<br><br>20. Verificar el impacto que los cambios en la tecnología puedan ocasionar a la seguridad, y si estos cambios la afectaran, dirigir la transición hacia un nuevo entorno de garantía.<br><br>21. Verificar los procedimientos usados para evaluar las políticas en la destrucción de la información, especificando los medios a utilizar, procedimientos a aplicar, y la oportunidad en que se ejecutará. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SOPORTE (SO)**<br><br>**SO1: MANTENIMIENTO DE HARDWARE.**<br><br>1. Verificar que existan contratos de mantenimiento preventivo y correctivo para el equipo informático de la institución.<br><br>2. Verificar si el mantenimiento otorgado por el proveedor es conforme a lo establecido en el contrato.<br><br>3. Verificar la programación del mantenimiento preventivo y correctivo, con la finalidad de reducir la frecuencia y el impacto de fallas de rendimiento.<br><br>4. Verificar cuál es el proceso de notificación de las fallas del equipo informático y como se documenta dicho proceso.<br><br>5. Verificar si el mantenimiento cubre la totalidad del equipo de cómputo o si es algún equipo especifico.<br><br>6. Verificar el tiempo de respuesta de reparación o sustitución de partes por medio del proveedor de servicio.<br><br>7. Verificar si el proveedor tiene la capacidad de ofrecer la sustitución temporal del equipo principal como servidores en caso de retiro por reparación u otro tipo de mantenimiento.<br><br>8. Verificar si existen informes sobre el mantenimiento a nivel físico y de parámetros efectuados por el proveedor a los servidores principales de la institución. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SO2: CONTROLES DE REDES Y COMUNICACIONES.**<br><br>1. Verificar que la Unidad de comunicaciones este integrada por el personal definido en el organigrama.<br><br>2. Verificar la existencia de un Inventario de direcciones IP asignada a los usuarios, con la información general asociada a cada IP.<br><br>3. Verificar la existencia de un inventario actualizado de equipo de comunicaciones: Módems, Hubs, Terminales, Routers, Firewalls, etc.<br><br>4. Verificar el inventario del software instalado en la red, por ejemplo: sistema operativo, lenguajes, programas, paqueterías, utilerías y demás software institucional.<br><br>5. Verificar el diagrama de red para identificar las interconexiones internas y externas.<br><br>6. Verificar si las claves para el uso de los equipos se resguardan en sobre sellado o lacrado para alguna eventualidad fortuita.<br><br>7. Verificar la existencia de servicios de Intranet, Extranet e Internet.<br><br>8. Verificar el tipo de Protocolo utilizado, por ejemplo: SNA, Netbios, IPX, TCP/IP<br><br>9. Verificar la existencia de procedimientos de autorización para conectar nuevo equipo en la red.<br><br>10. Verificar el procedimiento para el uso de cualquier conexión digital con el exterior, como línea conmutada o dedicada.<br><br>11. Verificar si el plan de contingencia considera el respaldo y recuperación de los sistemas de comunicaciones. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 12. Verificar si existe control y monitoreo de las conexiones a fin de deshabilitar aquellas que no estén en uso.<br><br>13. Verificar la existencia de software de monitoreo de las conexiones remotas, de forma que se documenten los incidentes o interrupción del servicio comunicación.<br><br>14. Verificar la existencia de una política que controle el uso del equipo de redes en producción y los equipos de prueba.<br><br>15. Verificar los tipos de prueba usadas para validar la operación del equipo de redes y comunicaciones.<br><br>16. Verificar si disponen de reportes de incidentes, contingencias y circunstancia que afecten el funcionamiento de la red, conforme a la bitácora.<br><br>17. Verificar como controlan el tamaño de los paquetes y flujo de la velocidad en la red.<br><br>18. Verificar cuales son los tipos de componente de obstáculos que dispone el Firewall, por ejemplo: Ruteador Filtra-paquetes, Gateway a nivel de Aplicación, Gateway a nivel de circuito.<br><br>19. Verificar como esta definida la política del perímetro de los Firewalls para el uso de Internet.<br><br>20. Verificar si están consideradas la bases para el diseño decisivo del Firewall en uso de Internet, asignadas por el administrador de red: Posturas sobre la política de Firewall, política interna propia de la organización, costo financiero y secciones de configuración<br><br>21. Verificar si han considerado por el responsable de seguridad en redes algunas características de diseño que son usadas para hacer mas seguro un servidor de defensa, al respecto se citan: | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | | Referencia |
|---|---|---|
| 21.1 | Verificar que la plataforma de Hardware del servidor de defensa ejecuta una versión "segura" de su sistema operativo, diseñado específicamente para proteger los sistemas operativos vulnerables y garantizar la integridad del Firewall. | |
| 21.2 | Verificar que únicamente los servicios que el administrador de redes considera esenciales son instalados en el servidor de defensa. La lógica de operación es que si el servicio no esta instalado, este puede ser atacado. Generalmente, un conjunto limitado de aplicaciones Proxy tales como Telnet, DNS, FTP, SMTP, y autenticación de usuarios son instalados en este servidor. | |
| 21.3 | Verificar si la Autenticación adicional para que el usuario accese a los servicios Proxy, por medio del servidor de defensa es ideal para colocar un sistema fuerte de supervisión de autorización. Adicionalmente, cada servicio Proxy podrá requerir de autorización propia después que el usuario tenga acceso a su sesión | |
| 21.4 | Verificar que cada Proxy es configurado para soportar únicamente un subconjunto de aplicaciones estándar de un conjunto de comandos. Si un comando estándar no es soportado por la aplicación Proxy, es porque simplemente no esta disponible para el usuario. | |
| 21.5 | Verificar que cada Proxy esta configurado para dejar acceder únicamente a los servidores especificados en el sistema. Esto significa que existe un conjunto de características/comandos que podrán ser aplicados para un subconjunto de sistemas en la red protegida | |
| 21.6 | Verificar que cada Proxy mantiene la información detallada y auditada de todos los registros del tráfico, cada conexión, y la duración de cada conexión. El registro de audición es una herramienta esencial para descubrir y finalizar el ataque de un intruso. | |
| 21.7 | Verificar que cada Proxy es un programa pequeño y sencillo específicamente diseñado para la seguridad de redes. Este permite que el código fuente de la aplicación pueda revisar y analizar posibles intrusos y fugas de seguridad. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: | |
|---|---|---|
| INSTITUCIÓN: | FECHA FIN: | |
| AUDITOR: | FIRMA: | |
| **Áreas / Actividades** | | **Referencia** |
| 21.8 Verificar que cada Proxy es independiente de todas las demás aplicaciones Proxy en el servidor de defensa. Si ocurriera un problema con la operación de cualquier Proxy, o si se descubriera un sistema vulnerable, este puede desinstalarse sin afectar la operación de las demás aplicaciones. Aun, si la población de usuarios requiere el soporte de un nuevo servicio, el administrador de redes puede fácilmente instalar el servicio Proxy requerido en el servidor de defensa | | |
| 21.9 Verificar si el Proxy generalmente funciona sin acceso al disco lo único que hace es leer su archivo de configuración inicial, desde que la Aplicación Proxy no ejecuta su acceso al disco para soporte, un intruso podrá encontrar más dificultades para instalar caballos de Troya perjudiciales y otro tipo de archivos peligrosos en el servidor de defensa. | | |
| 21.10 Verificar que cada Proxy corre como un usuario no- privilegiado en un directorio privado y seguro del servidor de defensa | | |
| 22. Verificar la disponibilidad de licencias y permisos de instalación. | | |
| 23. Verificar que los equipos de comunicación dispongan de claves de acceso, así como la activación de lóg. o bitácoras de auditoría sobre los accesos realizados. | | |
| 24. Verificar si han considerado en análisis y diseño el modelo de comunicación OSI de la red, en cuento a las uso de las capas: físicas, enlace, red, transporte, sesión, presentación y aplicación. | | |
| 25. Verificar como se evalúa la confiabilidad en el funcionamiento de los medios de transmisión y del medio físico que utiliza para las comunicaciones. | | |
| 26. Verificar que técnicas de transmisión se usan para la comunicación de la red, tales como: síncrona, asíncrona, analógica, digital, serie o paralelo. | | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 27. Verificar el funcionamiento y la confiabilidad de los dispositivos para conectar las redes, tales como: Repetidores, Puentes, Enrutadores y Puertas de enlace.<br><br>28. Verificar que mecanismos de funcionamiento usan en las técnicas de transferencias: Simples, Semidúplex, Dúplex total.<br><br>29. Verificar que tipo de topologías utilizadas para el diseño y uso de la red, por ejemplo: Bus, Estrella, Anillo, Malla, Doble anillo.<br><br>30. Verificar el medio usado para la conexión de los dispositivos a los servidores principales.<br><br>31. Verificar el uso de los servidores dedicados, de soporte, no dedicados, de impresión y de comunicación.<br><br>32. Verificar el número y características de las estaciones de trabajo así como los tipos de nodo en la red.<br><br>33. Verificar el tipo de cable utilizado en la red, tales como: trenzado, coaxial, de base para un canal, banda ancha o fibra óptica.<br><br>34. Verificar que elementos tienen definidos para la expansión de la red, considerar: Repetidores (para recibir y trasmitir datos), puentes (capa de enlace OSI para el manejo de datos origen y destino), Enrutadores (relacionado a los Protocolos de comunicación), puertas de enlace (dispositivos para la conexión de computadores y mainframe). | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SO3: CONTROL DE ALMACENAMIENTO.**<br><br>1. Verificar si la cintoteca se encuentra ubicada en el mismo edificio o en otro.<br><br>2. Verificar si los locales asignados a la cintoteca disponen de: Aire acondicionado, protección contra el fuego, cerradura de puerta especial ( tarjeta electrónica, acceso biométrico, cerradura eléctrica, etc. )<br><br>3. Verificar e identificar las características del hardware usado para la creación de las copias.<br><br>4. Verificar e identificar el software usado para la creación de las copias de respaldo.<br><br>5. Verificar si la institución dispone de algún software para el control de cintas utilizadas.<br><br>6. Verificar que el inventario de la cintoteca contiene información mínima como: Número de serie, número o clave del usuario, número del archivo lógico, nombre del sistema que lo genera, fecha de expedición del archivo, número de volumen, etc.<br><br>7. Verificar con qué frecuencia se validan los inventarios de los archivos magnéticos.<br><br>8. Verificar que procedimientos utilizan para copiar: documentos, datos, programas, reportes, etc. y si éstos están documentados.<br><br>9. Verificar si en el proceso de copiado de la información utilizan procesos de encriptamiento y autenticación.<br><br>10. Verificar la periodicidad con la que realizan pruebas de restauración de los medios magnéticos con la finalidad de asegurar la recuperación. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 11. Verificar si disponen de procedimientos que permitan la reconstrucción de un archivo el cual fue inadvertidamente destruido.<br><br>12. Verificar si identifican en la viñeta del medio magnético la información de carácter confidencial.<br><br>13. Verificar si existe un control estricto de las copias de archivos de carácter confidencial.<br><br>14. Verificar si borran los archivos de los dispositivos de almacenamiento, cuando se desechan, por inservibles.<br><br>15. Verificar si existe certificación de la destrucción de dispositivos magnéticos.<br><br>16. Verificar que medidas de control utilizan en caso de extravío de algún dispositivo de almacenamiento.<br><br>17. Verificar si existe restricción de acceso al lugar donde se mantiene la custodia de los medios magnéticos.<br><br>18. Verificar el control para registrar los medios magnéticos que se prestan y la fecha en que serán devueltos.<br><br>19. Verificar el procedimiento utilizado para el reemplazo o actualización de medios magnéticos. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SO4: SEGURIDAD FÍSICA.**<br><br>1. Verificar el cumplimiento de lo establecido en las normas de seguridad de acceso al centro de cómputo implementadas por TI.<br><br>2. Verificar que exista formulario de registro para el ingreso al centro de cómputo, para el personal externo al área.<br><br>3. Verificar que exista un sistema automático de extinción de fuego en el centro cómputo.<br><br>4. Verificar si los rociadores de agua, son del tipo de pre-acción cuya agua es suministrada con una cisterna, y que se activan a la primera alarma de incendio y se liberan por el mismo fuego, excepto la sala de cómputo.<br><br>5. Verificar la existencia de detectores de fuego y humo tanto en el área del techo y piso falso.<br><br>6. Verificar si en caso de una falsa alarma es posible de forma manual cortar la liberación automática de productos químicos extintores del fuego.<br><br>7. Verificar si estratégicamente existen extinguidores portátiles cerca del centro de cómputo, al nivel del suelo y marcados con una franja roja del suelo al techo.<br><br>8. Verificar que el sistema de alarma contra incendio automático tiene la capacidad de transmitir señales a un punto remoto que sea supervisado las 24 horas. El punto remoto puede ser una estación de guardia de la organización o la estación de bomberos local.<br><br>9. Verificar si los extintores instalados para fuego son de tipo automático ó manual. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar si el personal se encuentra capacitado para el uso y manejo de extintores. | |
| 11. Verificar si existe supervisión sobre la periodicidad de las cargas de los extintores conforme a lo recomendado por el proveedor. | |
| 12. Verificar si existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal pueda según el caso: cortar la acción, cortar la energía eléctrica, desalojar el edificio, etc. | |
| 13. Verificar que el papel y otros suministros combustibles se almacene fuera del centro de cómputo, a excepción de aquellos que se van a utilizar inmediatamente. | |
| 14. Verificar si existe un programa de capacitación para el personal, contra incendio y para la evacuación ordenada, en caso que se active la alarma de fuego. | |
| 15. Verificar si se prohíbe fumar, comer y beber dentro del centro de cómputo. | |
| 16. Verificar si existe vigilancia en el área de TI las 24 horas. | |
| 17. Verificar si ha instruido al personal de seguridad sobre las medidas a tomar en caso de que alguien pretenda entrar sin autorización, al área de TI. | |
| 18. Verificar si las visitas y demostraciones en el centro de cómputo, son controladas. | |
| 19. Verificar si se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas. | |
| 20. Verificar si existe vigilancia de la moral y comportamiento del personal de TI con el fin de mantener una buena imagen y evitar un posible fraude. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| | |
| **SO5: INFRAESTRUCTURA**<br>1. Verificar si la administración dispone de planos del edificio, con la finalidad de visualizar su distribución para identificar riesgos para el equipo informático.<br>2. Verificar que la construcción del edificio, incluyendo las paredes, techo y pisos, son de materiales no inflamable, como medida de reducir la posibilidad de incendio.<br>3. Verificar que las paredes se extiendan desde la estructura del piso a la del techo del edificio y no desde pisos elevados a techos falsos.<br>4. Verificar que la sala de cómputo se encuentre separada físicamente de otros departamentos de la organización.<br>5. Verificar si el edificio del centro de cómputo se encuentre en un nivel adecuado con la finalidad de minimizar el riesgo de un acceso externo o daño por inundación.<br>6. Verificar la existencia de una bóveda o caja fuente con puerta de seguridad de cierre automático con resistencia al agua y fuego, para el resguardo de medios magnéticos.<br>7. Verificar que la construcción del techo está a prueba de agua de forma que no fluya a los pisos inferiores.<br>8. Verificar que el drenaje sea adecuado en pisos elevados y estos posean desnivel.<br>9. Verificar que las puertas de entrada y salida del área de TI dispongan de un mecanismo que permita abrirlas en caso de emergencia. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 10. Verificar que las cortinas, muebles, piso y techo falso son de materiales no combustibles.<br><br>11. Verificar cada cuanto tiempo se realiza limpieza bajo el piso falso.<br><br>12. Verificar la existencia de mecanismos de cierre manual o automático de los ductos de aire acondicionado y ductos de aire fresco para el centro de cómputo. Esto cortará el flujo de aire en el área de proceso en caso de incendio de manera que no se alimenten las llamas.<br><br>13. Verificar la existencia de un sistema de potencia ininterrumpirle de energía y/o un generador diesel. Debido a que estos sistemas pueden ofrecer una protección temporal que permita la continuidad del servicio en caso falla de la energía eléctrica, o bien pueden ofrecer un respaldo eléctrico a largo plazo.<br><br>14. Verificar la existencia de protección contra variaciones de voltaje a toda la potencia eléctrica que se suministra a la unidad central de proceso y al equipo de comunicación.<br><br>15. Verificar si existe protección de todos los circuitos de la computadora contra actos de vandalismo que se puede dar cuando alguien abre los tableros de los circuitos y corta la energía. Esto implica el proveer tableros con cerraduras para los controles del circuito y el situarlos en habitaciones cerradas.<br><br>16. Verificar que el panel de la distribución del sistema eléctrico esté en un área segura e inaccesible a personas no autorizadas.<br><br>17. Verificar que los tableros del circuito se encuentren marcados de manera que al brindar mantenimiento, permitan una referencia rápida y expedita.<br><br>18. Verificar la existencia de lámparas de emergencia en el centro de cómputo. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 19. Verificar que abajo del piso se encuentran las líneas eléctricas por la seguridad del personal.<br><br>20. Verificar el medio ambiente que la temperatura y humedad del centro de cómputo esté en rango de 18℃ a 22℃<br><br>21. Verificar si el centro de cómputo dispone de aire acondicionado independiente del edificio central. | |
| | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SUBCONTRATACIÓN (SC)**<br><br>**SC1: EVALUACIÓN DE CONTRATOS DE SERVICIOS**<br><br>1. Solicitar una copia de los contratos de servicios proporcionados por terceros.<br><br>2. Identificar y analizar las condiciones pactadas en cada cláusula de los contratos de prestación de servicios de TI.<br><br>3. Identificar si existe cláusula de acuerdos de seguridad sobre reserva y confidencialidad de la información proporcionada por la institución y lo que resulte como producto del contrato.<br><br>4. Verificar la fecha del contrato, vigencia del contrato, y que sea firmado por la Alta Administración de la institución.<br><br>5. Condiciones mínimas a considerar dentro del contrato:<br>5.1 Título o nombre del contrato<br>5.2 Objeto del contrato de servicio<br>5.3 Medidas de desempeño<br>5.4 Presentación de informes de trabajos realizados<br>5.5 Resolución de diferencias y jurisdicción.<br>5.6 Incumplimiento y rescisión<br>5.7 Propiedad y Acceso<br>5.8 Planificación en caso de contingencia<br>5.9 Derechos de auditoría<br>5.10 Subcontratación o dependencia de otros<br>5.11 Confidencialidad/seguridad/separación de propiedades<br>5.12 Monto de los servicios, objeto del contrato, forma de pago y tipo de moneda<br>5.13 Seguros / Garantías<br>5.14 Ubicación física de la documentación.<br>5.15 Revisiones periódicas a los acuerdos | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| 6. Identificar las razones que llevaron a la suscripción del servicio:<br>6.1 Descentralizar operaciones<br>6.2 Liberar recursos para otros proyectos<br>6.3 Hardware o software obsoleto ó no actualizado.<br>6.4 Falta de Personal capacitado para efectuar funciones o procesos<br>6.5 Reducción de costos<br>6.6 Ampliación de operaciones.<br>6.7 Para ofrecer nuevos servicios a los clientes<br>6.8 Procesamiento general de redundancias y contingencias<br>6.9 Compromisos estratégicos<br>6.10 Cumplimiento legal o normativo<br>6.11 Cumplimiento de plazos críticos<br>6.12 Fusiones, adquisiciones e integración de servicios.<br>6.13 Minimizar riesgos<br><br>7. Verificar que la gerencia de TI haya establecido un proceso de monitoreo continuo sobre la prestación de servicios contratados, con el fin de asegurar el cumplimiento de las cláusulas del contrato.<br><br>8. Verificar que el contrato haga referencia a los anexos de especificaciones técnicas y plan de ejecución entre otros. | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SC2: EVALUACIÓN DEL PROVEEDOR.**<br><br>1. Identificar si el proveedor es nacional o internacional, con el objetivo de obtener información sobre: tipo de representación, ubicación física, personal de enlace, teléfonos, etc.<br><br>2. Verificar si entre los criterios para elegir al proveedor del servicio se considera:<br>2.1 Experiencia en procesos/servicio.<br>2.2 Tamaño y situación financiera.<br>2.3 Confiabilidad e historial.<br>2.4 Conocimiento del mercado.<br>2.5 Soporte técnico.<br>2.6 Cultura corporativa<br>2.7 Referencias institucionales.<br>2.8 Cumplimiento de leyes y normas.<br>2.9 Costos / competencia<br>2.10 Tiempos de respuesta ante eventos programados e imprevistos<br>2.11 Soporte post- implementación.<br>2.12 Garantía sobre productos y servicios | |

| PROGRAMA DE AUDITORÍA DE SISTEMAS | FECHA INICIO: |
|---|---|
| INSTITUCIÓN: | FECHA FIN: |
| AUDITOR: | FIRMA: |

| Áreas / Actividades | Referencia |
|---|---|
| **SC3: EXAMEN DE LOS SERVICIOS SUBCONTRATADOS.**<br><br>1. Verificar que exista una persona responsable en el área de TI, que controla la calidad de los productos y/o servicios prestados por el proveedor.<br><br>2. Verificar si todas las relaciones del servicio con el proveedor están garantizadas con un contrato formal.<br><br>3. Verificar si el proveedor ha subcontratado parcial o total los servicios que proporciona la institución y qué controles tiene sobre estos.<br><br>4. Identificar el riesgo de dependencia de la institución hacia el proveedor de servicios y el impacto de éste en las operaciones diarias.<br><br>5. Identificar si existe un análisis de los principales riesgos en la subcontratación:<br>5.1 Documentación técnica.<br>5.2 Procesamiento de transacciones y operaciones<br>5.3 Energía eléctrica, comunicaciones y redes<br>5.4 Servicio al cliente<br>5.5 Planes para la continuidad/reanudación de las operaciones<br>5.6 Apoyo a sistemas y operaciones (consultas- soporte)<br>5.7 Planificación, ejecución y administración de proyectos<br>5.8 Seguridad informática y privacidad de la información de la empresa y de los clientes que implica riesgos legales, normativos y de reputación en las jurisdicciones del cliente-anfitrión.<br>5.9 Eventos externos (desastres naturales/disturbios, etc.) que restringen la movilidad del personal y el acceso a las instalaciones de procesamiento | |