ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA
ESPECIALIZACIÓN EN GERENCIA INFORMÁTICA
ASIGNATURA: Auditoría de Sistemas

CORPORACIÓN UNIVERSITARIA REMINGTON
DIRECCIÓN PEDAGÓGICA

2011

CRÉDITOS

AUTOR

Elizabeth Díaz Duque
Ingeniera de Sistemas de la Universidad EAFIT Medellín
Especialista en Pedagogía de la Virtualidad de la Fundación Universitaria Católica del Norte
Diplomatura en Ambientes Virtuales de Aprendizaje
Jefe de Área de Informática y Tecnología del Colegio Gimnasio Los Pinares de Medellín, docente durante los últimos 5 años ediazduque@gmail.com

Nota: el autor certificó (de manera verbal o escrita) No haber incurrido en fraude científico, plagio o vicios de autoría; en caso contrario eximió de toda responsabilidad a la Corporación Universitaria Remington, y se declaró como el único responsable.

RESPONSABLES

Jorge Mauricio Sepúlveda Castaño
Director del programa Escuela de Ciencias Básicas e Ingeniería

Director Pedagógico
Octavio Toro Chica
dirpedagogica.director@remington.edu.co

Coordinadora de Medios y Mediaciones
Angélica Ricaurte Avendaño
mediaciones.coordinador01@remington.edu.co

GRUPO DE APOYO

Personal de la Unidad de Medios y Mediaciones
EDICIÓN Y MONTAJE
Primera versión. Febrero de 2011.

TABLA DE CONTENIDO

1. MAPA DE LA ASIGNATURA

AUDITORÍA DE SISTEMAS

PROPÓSITO GENERAL DEL MÓDULO

Con este módulo de trabajo se pretende hacer una introducción a los estudiantes hacia el concepto de "auditorías" en el campo de los diferentes sistemas, y que a través de las ejemplificaciones expuestas, los educandos pueden tener una idea general de cómo se evalúan a las organizaciones en el departamento de sistemas.

OBJETIVO GENERAL

Introducir a los estudiantes en el contexto de un sistema, y que comprenda el concepto de valoración de las fortalezas y debilidades del mismo y que sea capaz del diseño de controles que eviten posibles errores, preservando el correcto alcance de los objetivos del sistema

OBJETIVOS ESPECÍFICOS

- Conocer los instrumentos básicos que permitan la detección de debilidades y posibles riesgos en los diferentes Sistemas de una organización.
- Comprender cómo se lleva a cabo una auditoría de acuerdo con las directrices de las Auditorias de Sistemas generalmente aceptadas para que la tecnología de información de la organización y los sistemas empresariales sean adecuadamente controlados, vigilados y evaluados.
- Evaluar las directrices para una auditoría de sistemas, además de su aplicabilidad en una organización

UNIDAD 1	UNIDAD 2	UNIDAD 3
QUÉ ES LA AUDITORÍA DE SISTEMAS -DESARROLLO CONCEPTUAL-	OBJETIVOS GENERALES DE LA AUDITORÍA DE SISTEMAS -DESARROLLO CONCEPTUAL-	AUDITORÍAS DE SISTEMAS -ESTUDIO DE CASOS APLICABLES-

2. UNIDAD 1 ¿QUÉ ES LA AUDITORÍA DE SISTEMAS?

OBJETIVO GENERAL

Conocer los instrumentos básicos que permitan la detección de debilidades y posibles riesgos en los diferentes Sistemas de una organización.

OBJETIVOS ESPECÍFICOS

- Introducir a los estudiantes al concepto general de la auditoría de sistemas.
- Plantear los conceptos generales de una auditoría de sistemas para contextualizar a los estudiantes en dicho campo.
- Presentar el papel o rol principal de un auditor de sistemas en los procesos de auditorías.

Prueba Inicial

Resuelve el siguiente acertijo, El acertijo dice así:
Tenemos 5 casas de cinco colores diferentes y en cada una de ellas vive una persona de una nacionalidad diferente.

Cada uno de los dueños bebe una bebida diferente, fuma una marca de cigarrillos diferente y tiene una mascota diferente.

Tenemos las siguientes claves:

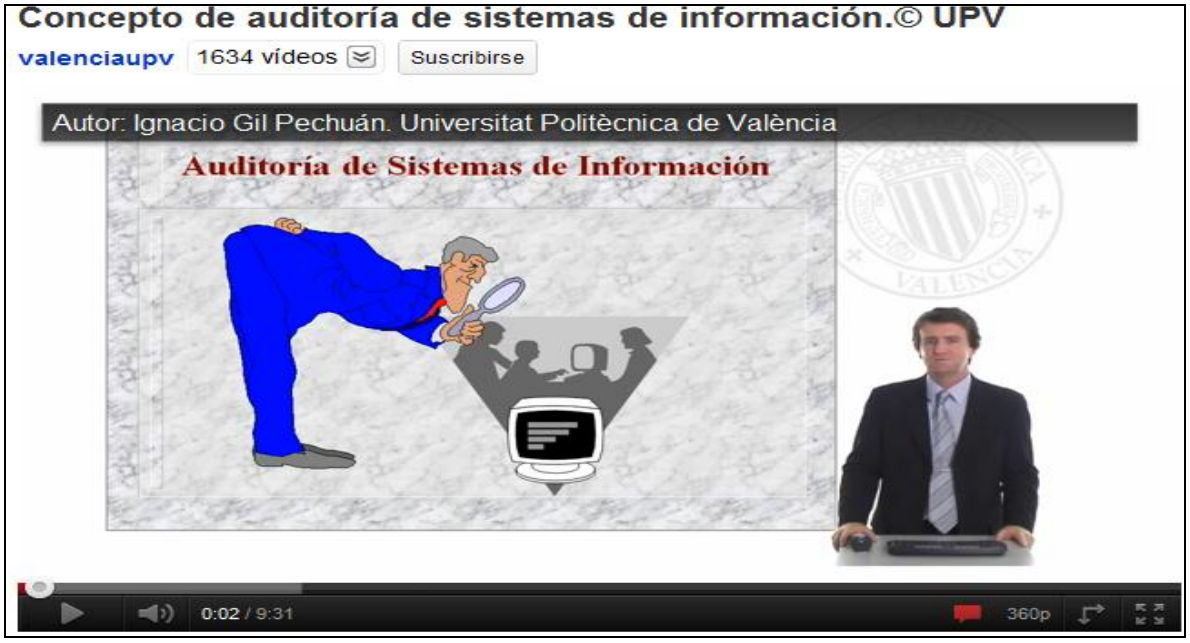
- El británico vive en la casa roja.
- El sueco tiene un perro.
- El danés toma té.
- La casa verde está a la izquierda de la blanca.
- El dueño de la casa verde toma café.
- La persona que fuma Pall Mall tiene un pájaro.
- El dueño de la casa amarilla fuma Dunhill.
- El que vive en la casa del centro toma leche.
- El noruego vive en la primera casa.
- La persona que fuma Brends vive junto a la que tiene un gato.
- La persona que tiene un caballo vive junto a la que fuma Dunhill.
- El que fuma Bluemasters bebe cerveza.
- El alemán fuma prince.

- El noruego vive junto a la casa azul.
- El que fuma Brends tiene un vecino que toma agua.

Y por último la pregunta: ¿Quién es el dueño del pececito?

TEMAS

Antes de comenzar, veamos el siguiente video como introducción a la Unidad



Video Intro unidad 1
En: http://www.youtube.com/watch?v=IgN3hrS5rJ4

1. **¿QUÉ ES LA AUDITORÍA DE SISTEMAS?**

a. DEFINICIÓN
b. CONCEPTOS GENERALES
c. ROL DEL AUDITOR DE SISTEMAS

2. **OBJETIVOS DE UNA AUDITORÍA DE SISTEMAS**

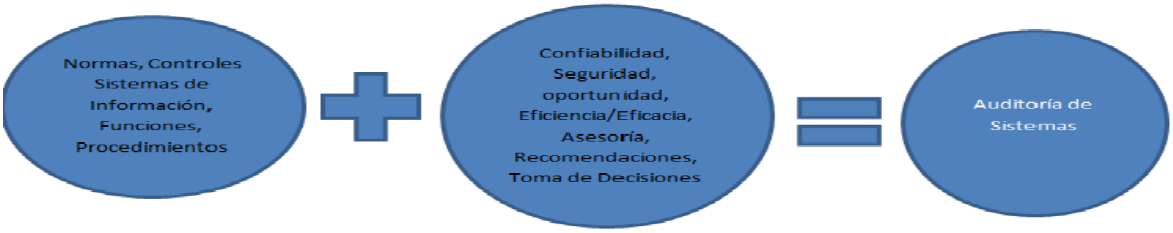
3. **LA FUNCIÓN DE LA AUDITORÍA EN LA ORGANIZACIÓN**

2.1. ¿Qué es la auditoría de sistemas?

¿QUÉS LA AUDITORÍA DE SISTEMAS?

a. DEFINICIÓN:

Si entráramos a definir el concepto de auditoría, comenzaríamos por definirlo desde su raíz, así, la palabra "auditoría", proviene del latín auditor, -ōris y así mismo ésta nos trae a colación la palabra "auditor", que es aquella persona que se encarga de hacer las auditorías haciendo uso de una de las mayores virtudes que éste debe tener y es: "oir", pues así podrá realizar su trabajo de revisión de acuerdo a un objetivo específico que debe ir incluido en todo proceso de auditoría y es el de evaluar la eficiencia y la eficacia con la que se está realizando cualquiera procedimiento y así la organización pueda tomar las decisiones pertinentes que permitan corregir los errores, en caso de que existieran, o así también mejorar el desarrollo de dicho procedimiento.



Definición de Auditoría Sistemas

b. CONCEPTOS DE LA AUDITORÍA DE SISTEMAS

Comencemos por definir algunos conceptos que se deben tener en cuenta para el entendimiento de las auditorias de sistemas.

SISTEMA: entendido como el conjunto de elementos, o reglas de una materia en específico que están enlazadas entre sí de una manera lógica- racional. Algunos ejemplos podrían ser: Sistema nervioso, Sistema Numérico, Sistema de Información.

INFORMACIÓN: la información en general podríamos definirla como un conjunto de datos organizado que conlleva un mensaje.

No puede confundirse la información con los Datos, pues estos son realmente una simple representación simbólica de una entidad cualquiera, pero que por sí sólo no representa un mensaje.

Consideremos los siguientes ejemplos:

Datos: Ana, Restrepo/ 15 años/ Bogotana
Información: Ana Restrepo tiene 15 años y su ciudad de procedencia es Bogotá.

PROCESO: Entendido como un conjunto de actividades coordinados entre sí, que suceden de acuerdo a un fin común.

Ejemplo: Proceso de Selección de Personal

PROCEDIMIENTO: este concepto podríamos definirlo como el "modo o la manera" de ejecutarse las diferentes acciones o actividades de un proceso. Desde el campo de la computación podríamos llamarlo como una "subrutina".

Ejemplo: Registro de la documentación en la oficina de reclutamiento de personal.

EVALUACIÓN: consideremos ésta como aquella acción encargada de darle la estimación o grado de valor a algo.
Consideremos también que no todo es medible desde el campo numérico, pero si desde lo cualitativito puede darse una estimación a lo evaluado.

Ejemplos: Numérica→el 80% del personal está a gusto con el servicio recibido.
Cualitativa→El servicio fue evaluado como "muy bien prestado".

VERIFICACIÓN: es entendida como aquella acción que permite examinar y comprobar la verdad o validez de algo.

Ejemplo: Se considera un número par, a todo aquel que puede ser divisible por dos (2) y su resultado es una división exacta. Luego el número 10 es par. Verificación→ 10/2=5.

c. ROL DEL AUDITOR DE SISTEMAS:

Si partimos que la auditoría de sistemas debe tener como fin la evaluación y análisis de los procesos informáticos, luego, debemos entender entonces el papel o rol de dicho auditor de sistemas como el ente evaluador que debe estar atento a identificar los problemas o posibles problemas que puedan estar presentes dentro de los sistemas utilizados en la organización, pero así mismo debe estar abierto a proponer soluciones a estos mismos.

Es indispensable que este auditor de sistemas tenga formación en los siguientes aspectos:
Analizar cuando y como los medios de la organización auditada pueden conseguir su máxima eficacia. Por ende debe presentar por escrito sus propias recomendaciones del estudio realizado, además de las posibles soluciones, de acuerdo a los problemas detectados en dicho sistema informático.

Luego de esto, el auditor debe establecer aquellos requisitos mínimos, para poder que se puedan adecuar y por ende permitir las funciones para las cuales fue diseñado dicho sistema y éste pueda cumplir con lo requerido.

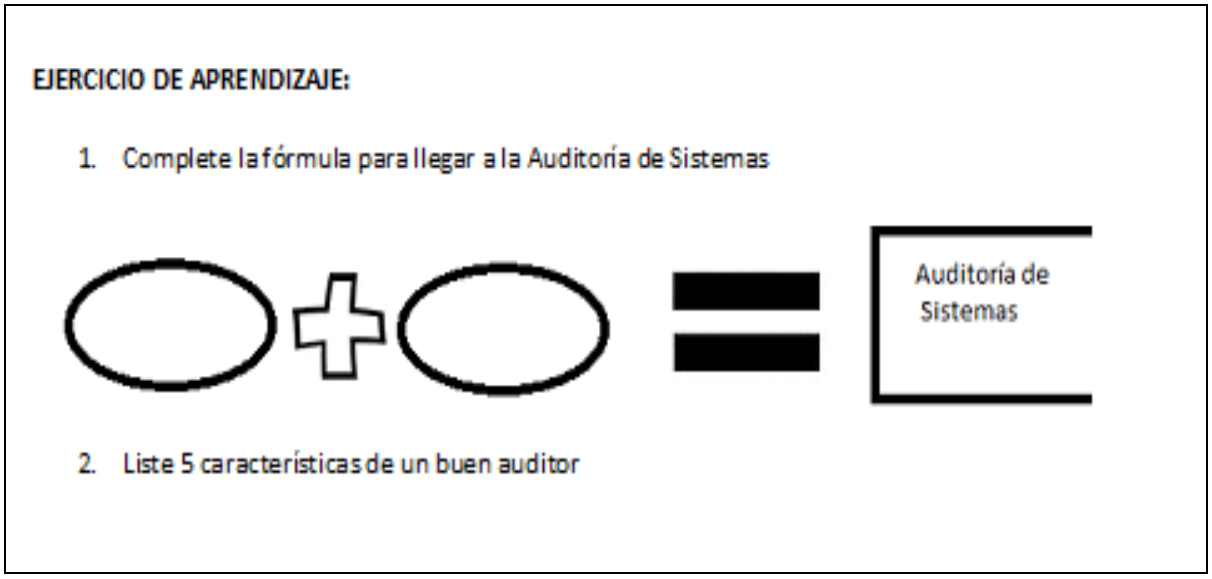
Cabe anotar que el auditor debe abstenerse de dar recomendaciones a la organización, que sean de carácter innecesario o que puedan ser riesgosas o que carezcan de todo tipo de soporte.

El auditor además debe prestar su servicio de auditoría haciendo uso de las posibilidades a su alcance (medios), pero que siempre pueda asegurar que su trabajo puede ser ejercido con toda idoneidad. Si existe el caso que los medios no le permitan hacer su trabajo con total libertad, es necesario entonces que el auditor no realice dicha función de auditoría y sugiera un cambio de fecha para dicha auditoría hasta que la organización le garantice las condiciones mínimas necesarias para dicha actividad.

Si el auditor encontrara un caso de auditoría en el cual él considere que sus conocimientos no son los suficientes para la materia en evaluación, éste deberá buscar un experto en la materia y remitir su informe para poder analizarlo en condiciones idóneas y así poder reforzar la calidad de la auditoría.

El auditor debe facilitar e incentivarla confianza con el/los auditados basándose en una actuación enteramente transparente, y manejando un perfil humilde que le permita al auditado mostrar sus resultados sin ningún temor, y así asegurar un proceso de auditoría con calidad.

Ejercicio

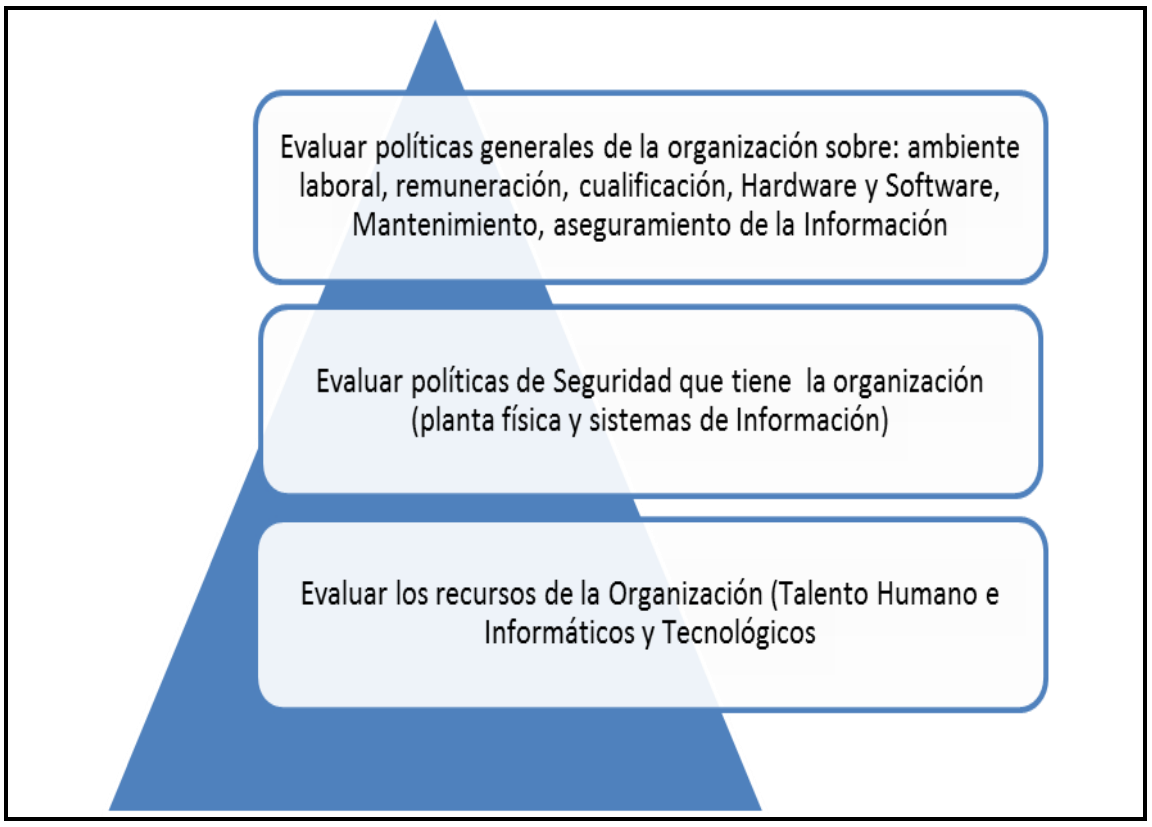


2.2. Objetivos Generales de la Auditoría de Sistemas

2. OBJETIVOS GENERALES DE LA AUDITORÍA DE SISTEMAS

Veamos algunos de los objetivos que la auditoría de sistemas debe plantearse siempre. Cabe aclarar que estos son los objetivos generales de la auditoría, los específicos ya van estrictamente ligados al proceso específico a evaluar/auditar:

- Evaluar las políticas generales acerca del ambiente laboral, desempeño, planeación, capacitación y cualificación, motivación y remuneración del personal de la organización.
- Evaluar las políticas que tiene la organización con respecto al software, hardware, desarrollo y mantenimiento de los sistemas de información.
- Evaluar las políticas de la organización que tienen con respecto a la seguridad tanto de la planta física, como de respaldo de la información.
- Evaluar los recursos tecnológicos e informáticos de la organización.
- Analizar cómo se concibe dentro de la organización la implementación y funcionalidad del sistema de aseguramiento de la información.



Objetivos Generales de la Auditoría

EJERCICIO DE APRENDIZAJE:

Haga una lista de 5 objetivos que pretenda alcanzar la auditoría planeada en la organización.

2.3. La Función de la Auditoría en la Organización

3. LA FUNCIÓN DE LA AUDITORÍA EN LA ORGANIZACIÓN

- Para definir la función que tienen las auditorías en la organización, recordemos entonces que la auditoría tiene como fin evaluar y tratar de controlar los sistemas informáticos para poder protegerlos, además de verificar que las actividades de dichos sistemas si se desarrollen bajo las normas informáticas generales existentes y así poder asegurar la eficacia que la organización espera, pues no podemos aislar los sistemas de información del control respectivo al que se someten los demás procesos de la organización.

Entendamos entonces porqué es importante la auditoría de sistemas dentro de la organización, a partir de la contemplación de los siguientes aspectos:

- Los equipos de cómputo y centros de procesamiento de datos pueden ser bastante buscados bien sea para funciones de espías o para delinquir. Estos equipos al procesar y transmitir información podrían enviar paquetes de datos con errores tales como virus o archivos dañados. He ahí entonces una actividad que la auditoría puede ayudar a controlar y mejorar.

- Ahora, un sistema de información que esté mal diseñado e implementado puede ser una herramienta muy peligrosa para cualquier persona, ya que no podemos olvidar que las máquinas sólo reciben órdenes de una persona, y ya estos equipos (computadores) generan el material informático de cada organización. Por esto una organización no puede en ningún caso depender total o parcialmente de un programa (software) mal diseñado, o bien de equipos malos (hardware).

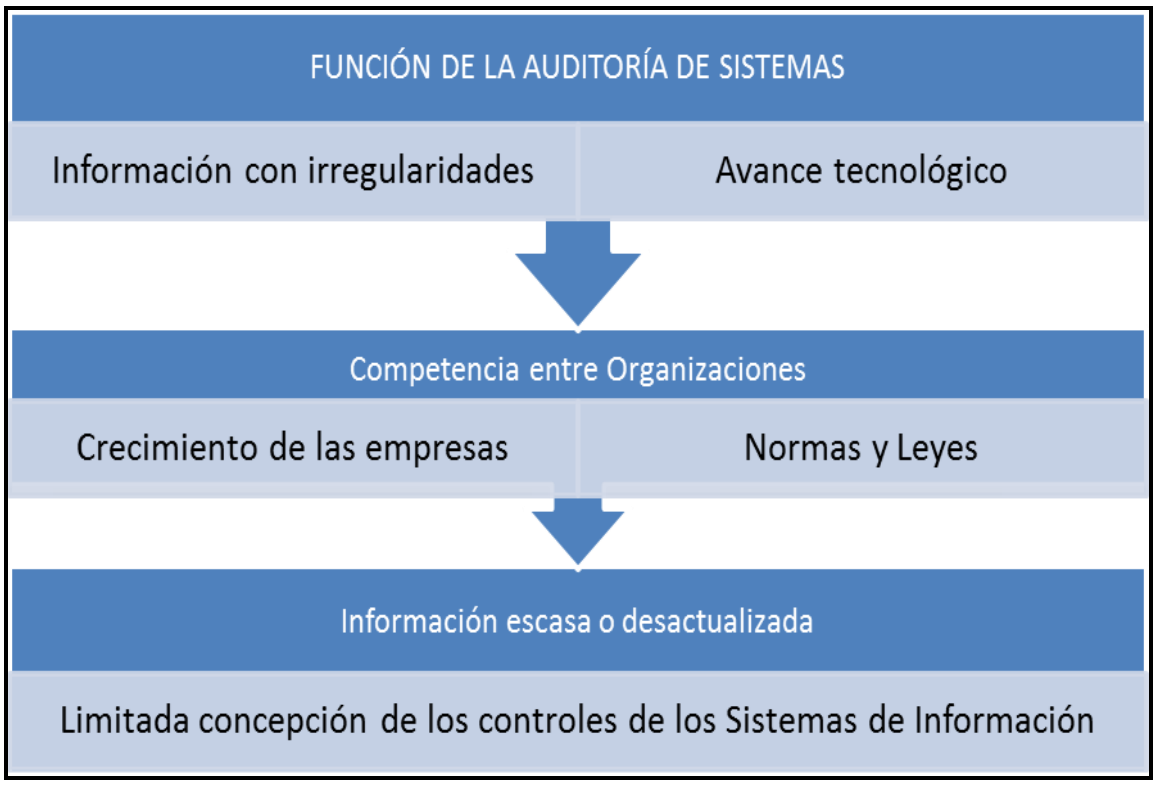
- De la misma manera que la tecnología va avanzando día a día, así mismo, las organizaciones deben ir avanzando y por ello es que se deben evaluar constantemente los controles aplicados a los sistemas y así haya una consolidación y coherencia con los cambios que se vivan dentro de la organización.

- El desarrollo de la auditoría de sistemas es bastante básico, ya que no cuenta con todos los recursos necesarios para ella, han hecho entonces que los controles ejercidos se vean solamente enfocados a los procesos donde el Software y el Hardware se vean involucrados.

- Es muy importante que las organizaciones aumenten sus controles y acciones de control frente a los sistemas de información, ya que las auditorías les muestran el alcance de seguridad de dichos sistemas, que están altamente centrados en la seguridad física.

- La auditoría de sistemas es de gran ayuda para la organización puesto que hoy es muy poca o en casos escasa la documentación de las organizaciones, o también información desactualizada, y los sistemas de información podrían subsanar este aspecto.

Veamos en el siguiente gráfico los aspectos principales que ayudaría la auditoría en cualquier organización.



Función Auditoría en la Organización

Ejercicio de aprendizaje

Defina en 5 líneas, 2 funciones básicas que cumpliría una auditoría en cualquiera organización.

3. UNIDAD 2 LA AUDITORÍA DE SISTEMAS

OBJETIVO GENERAL

Comprender cómo se lleva a cabo una auditoría de acuerdo con las directrices de las Auditorias de Sistemas generalmente aceptadas para que la tecnología de información de la organización y los sistemas empresariales sean adecuadamente controlados, vigilados y evaluados.

OBJETIVOS ESPECÍFICOS

- Introducir a los estudiantes en la planeación general y adecuada de una auditoría de Sistemas.
- Analizar los respectivos controles que maneja toda auditoría de sistemas.
- Conocer la metodología que debe tenerse en cuenta para que una auditoría de sistemas sea exitosa.

Prueba Inicial

En la Unidad 1 leíste lo que es una auditoría de Sistemas, escribe 5 actividades, que usted como auditor haría previamente a la realización de una auditoría.

Actividad 1: _____

Actividad 2: _____

Actividad 3: _____

Actividad 4: _____

Actividad 5: _____

3.1. Planeación de una Auditoría de Sistemas

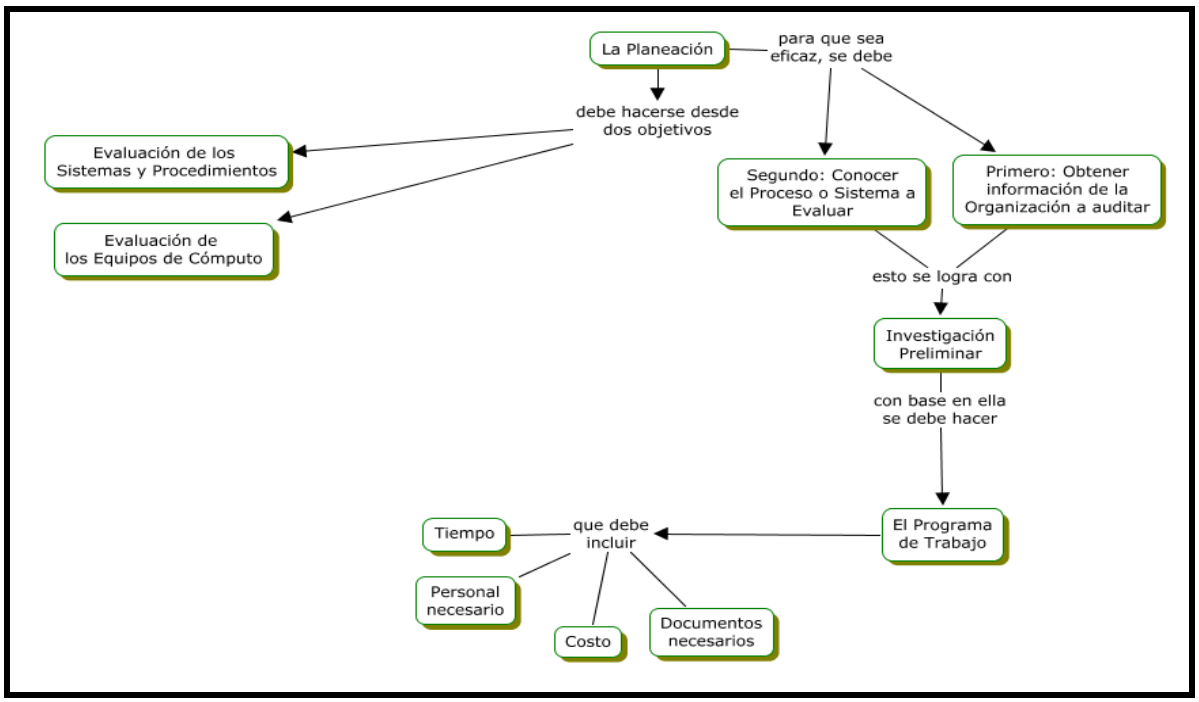
Veamos el siguiente video como abrebocas de la Unidad:
http://www.youtube.com/watch?v=9WMu6d-py2A

Video Intro Unidad2

Recordemos entonces que la auditoría de sistemas es la encargada de revisar y evaluar los sistemas, controles y procedimientos de los diferentes sistemas de la organización, además de los anteriores, también se incluye la inspección de los diferentes equipos de cómputo, su uso y la seguridad de los mismos, esto todo con el fin de buscar un uso más eficiente y seguro de toda la información que es la base para las decisiones de la organización.

Miremos entonces como se podría hacer una adecuada planeación de una auditoría de sistemas, y para esto es absolutamente necesario seguir una serie de pasos que vienen previos a la auditoría en sí, con el fin de lograr dimensionar las diferentes características del área a auditar dentro de la organización o ente auditado.

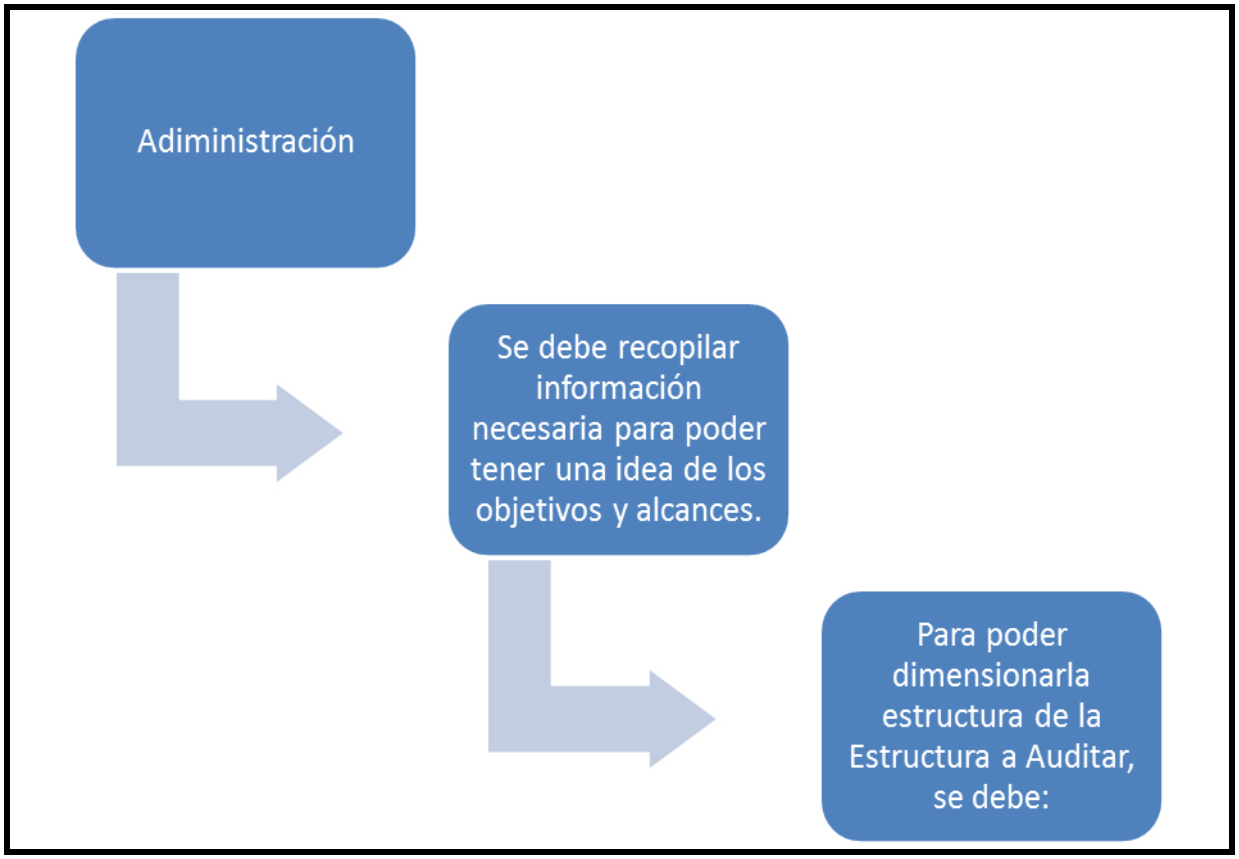
Veamos entonces, a través de la siguiente gráfica los primeros pasos que se debe tener en cuenta antes de una auditoría:



Pasos Previos a una Auditoría

Desglosemos el mapa anterior a partir de la "Investigación Preliminar", la cual consiste en explorar el estado general de área a auditar y su estado frente a la organización.

Además se debe hacerla investigación preliminar solicitando información de las diferentes áreas de la organización, y revisándola teniendo en cuenta aspectos como:



Investigación Preliminar

Ahora veamos que se necesita para Dimensionar la estructura a Auditar:

1. **En el Área de Sistemas:**

a. Objetivos a Largo plazo
b. Objetivos a Corto Plazo

2. **Recursos materiales: pedir documentos que evidencien información como**:

a. Número de equipos y sus características
b. Información de instalación de los equipos
c. Contratos de los equipos (comprar, alquiler, mantenimiento).
d. Políticas para el uso de los equipos
e. Información de los Seguros
f. Información de Ubicación de los equipos
g. Convenios existente con otras entidades
h. Planes de expansión

4. Información de la descripción general de los Sistemas

Que existen instalados en la Organización y también la de aquellos que están en lista de espera para ser instalados y que contengan información en ellos. Pare ello se debe solicitar documentación o soporte de información como:

a. Manual de Procedimiento de los Sistemas
b. Diagramas de entrada y salida (I/O)
c. Fechas de instalaciones
d. Planes de instalación a futuro

Muy bien, luego de solicitar esta información para el dimensionamiento de la Organización, podemos encontrar varios casos. Veámoslos:

CASO 1: La información solicitada No la tiene la Organización, y ésta se necesita

CASO 2: La información solicitada No se tiene y No se necesita

CASO 3: La Organización cuenta con la información, pero ésta está incompleta, desactualizada, inadecuada, no se usa.

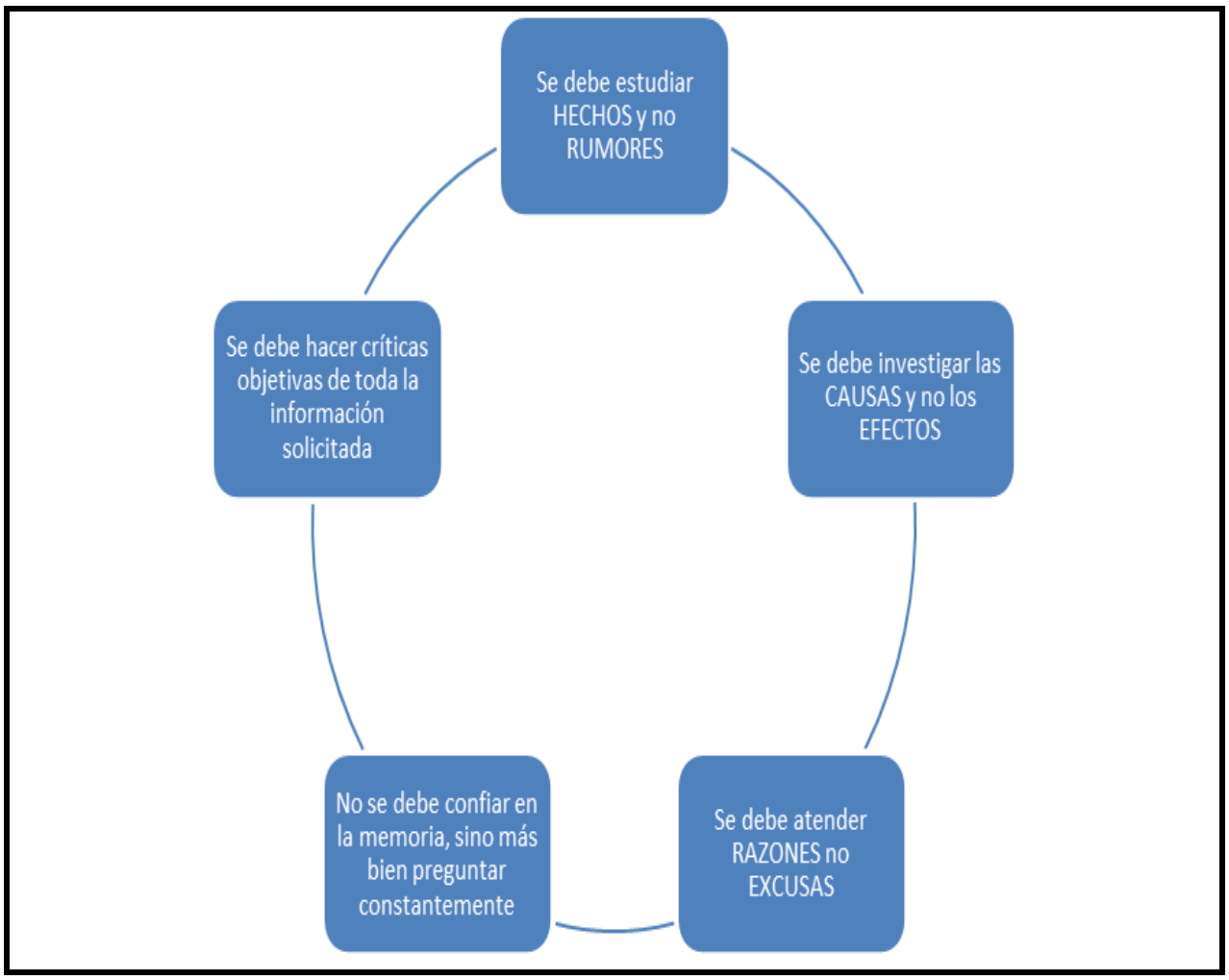
CASO 4: La información con la que se cuenta es la requerida, está actualizada, y es necesaria.

En el CASO 1, se debe analizar el POR QUÉ NO SE NECESITA.

En el CASO 2, se debe recomendar a la Organización la elaboración de ésta teniendo en cuenta las necesidades y el uso que se le daría a ésta.

En el CASO 3, al igual que en el caso 2, se deben hacer las recomendaciones necesarias para completar dicha información, o actualizarla, u orientar su uso.

El éxito para los análisis de la información requerida, depende de las siguientes recomendaciones que debemos tener en cuenta como auditores:



Recomendaciones para el auditor

EL PERSONAL PARTCIPANTE

Este es otro aspecto que es fundamental dentro de la planeación de una auditoría de sistemas, pues es el personal con sus características de quienes participan en estos procesos los que aseguran en gran parte el éxito de las auditorías.

En este caso, la mayoría del personal que se busca para la realización de los procesos de auditorías debe ser personal altamente capacitado, con valores éticos para ejercer su trabajo con rectitud y así mismo podérsele retribuir justamente por su trabajo.

Con estos requisitos mencionados anteriormente, además de considerar las características de sus buenos conocimientos, práctica y profesionalismo podríamos decir que se cuenta con un personal idóneo para intervenir en las auditorías.

No se puede olvidar que las organizaciones cuentan con muy buen talento humano que puede llevar a cabo los procesos de auditorías y poder proporcionar y programar las reuniones o las actividades necesarias o requeridas. Además que la alta gerencia debe garantizar al auditor, todo el apoyo necesario a través del uso de todo el personal multidisciplinario con el que cuente la organización para asistir en la actividades programas y poder garantizar la obtención de la información en el momento indicado.

También se debe contar con algún personal que sea discriminado por los diferentes usuarios del sistema, pues es necesario que cuando el auditor solicite diferentes tipos de información para el análisis de algunas de las premisas planteadas para dicha evaluación, se pueda contar con no sólo el punto de vista del área de sistemas, sino también de los mismos usuarios de estos sistemas.

Ahora veamos un ejemplo de personal con algunas de las características requeridas, que se sugiere para dicho trabajo:

- Un técnico en sistemas/Informática, con experiencia en dicha área, además de conocimiento y experiencia en el análisis de sistemas. Pero sobre todo conocimiento de los sistemas claves de la organización.

Ahora, si se viera involucrado el auditor en un caso de sistemas con alta complejidad, es indispensable contar con un experto bien sea den Telemática, Bases de Datos, u otras áreas afines.

EJERCICIO DE APRENDIZAJE:
1. Mencione y explique al menos 2 de los casos posibles que se pueden presentar en la solicitud de información en una auditoría.
2. Escriba 4 recomendaciones para un buen auditor.

3.2. Los Controles de una Auditoría

3.2.1. Definición de Controles

Podríamos definir los controles como todo aquel conjunto de técnicas, procedimientos que están interrelacionados con los sistemas de una organización entre sí permiten hacer una evaluación y corrección oportuna de aquellas actividades que no se estén ejecutando con tal eficiencia que se puedan alcanzar los objetivos del mismo.

Una de las razones por las cuales se implementaron los controles en el área de sistemas, se debe al gran crecimiento de la dependencia de las organizaciones de los diferentes componentes de esta área, esto es, de los equipos, de los programas, y del procesamiento de la información y como estos son manipulados por distintas personas, por ello el porcentaje de error en ellos necesita ser controlado a través de estas herramientas como son los controles.

Algunas de las características que deben tener los controles son:

- Éste debe ser ejecutado constantemente para poder encontrar los errores muy a tiempo y actuar o corregir oportunamente.
- Éste debe ser económico, es decir, sus resultados deben ser muchos mejores que los costos en los que pueda incurrir la institución al implementar estos sistemas de control.
- La información obtenida por los controles debe ser muy verídica, para que las correcciones no sean implementadas con base en ideas subjetivas.
- El control debe provenir de un sistema de planeación tan bien planeado que deje muy claro el alcance necesario para las acciones correctivas.
- El control no debe interferir en el desarrollo normal de la organización.

3.2.2. Clasificación de Los Controles

CONTROLES PREVENTIVOS

Estos consisten en aquellas herramientas que permiten disminuir la frecuencia con la que ocurren las fallas.

Ejemplo: las copias de seguridad o back up de la información.

- **CONTROLES DETECTIVOS**

Estos controles tienen una característica especial y es que no evitan las fallas, sólo las detectan. Estos son una gran herramienta para el auditor puesto que le permite la evaluación de los controles preventivos.

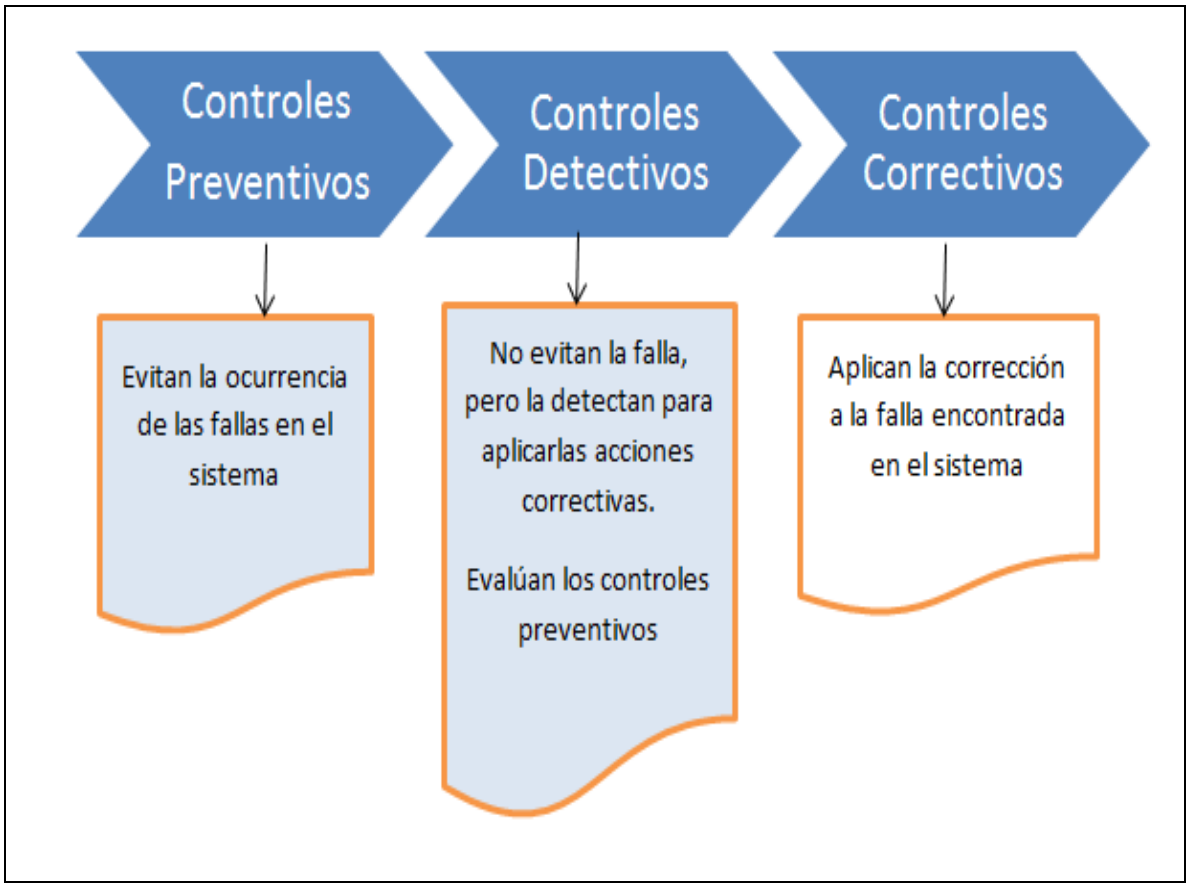
Ejemplo: El archivo o documento de las revisiones periódicas de los diferentes equipos de la organización, con el reporte de fecha de la copia de seguridad del mismo.

- **CONTROLES CORRECTIVOS**

Estos ayudan a la corrección e investigación de las causas de las fallas. La corrección en sí puede ser difícil e ineficiente en sí misma, pues la corrección de errores es una actividad con un porcentaje alto de errores en sí, por esto, es necesario en muchos casos aplicar controles detectivos en los mismos controles correctivos.

Ejemplo: Jornada de formación y capacitación sobre las posibles consecuencias futuras que le implica a la organización la falta en la realización de las copias de seguridad.

Observemos el siguiente gráfico que resume los diferentes tipos de controles:



Tipos de Controles

EJERCICIO DE APRENDIZAJE:

1. Defina en sus propias palabras lo que es un “control”.
2. Escriba 2 ejemplos de alguno de los tipos de controles.

3.3. Metodología de una Auditoría

Los diferentes errores en los diferentes sistemas de información de las organizaciones han causado conflictos entre las diferentes personas miembros de una organización o sección en específico de la misma, pues cuando estos sistemas se vuelven difíciles de operar, éstos hacen que así mismo se vuelvan muy complicado su desarrollo a futuro, haciendo que la organización no pueda gozar de los beneficios de un sistema de información.

De ahí entonces la necesidad de las auditorías de cada uno de los procesos de dichos sistemas de información. Pero para la consecución de este objetivo es totalmente necesaria una adecuada planeación y esto implica un trabajo riguroso y eficiente para evitar que se olviden aspectos fundamentales en la realización de dicho trabajo, además que se debe tratar de buscar la optimización de los recursos de todo orden (técnicos, humanos, económicos y logísticos).

Ahora veamos entonces como se podría orientar el trabajo que está envuelto en los procesos de auditorías. Algunas preguntas que nos podríamos realizar para buscar el norte del proceso, podrían ser:

- ¿Qué se debe hacer?
- ¿Qué voy a auditar?
- ¿Cuándo lo debo hacer?
- ¿Cómo lo debo hacer?
- ¿Qué recursos necesito?
- ¿Qué recursos tengo?

Todas estas preguntas ayudan a minimizar la improvisación, los desfases y a optimizar los diferentes recursos como lo habíamos dicho antes.

Ahora entremos a detallar algunos de los objetivos que están presentes en la auditoría de sistemas:

- Tener un plan de auditorías que permita tener claros los requisitos para que así la realización de las actividades del proceso de evaluación/ auditoría de manera que los costos sean los mínimos y que no se dupliquen esfuerzos.

- Ir comparando las actividades que se van ejecutando con aquellas que se planearon, pero esto se hace al tiempo que se va analizando si hay retrasos y se determinan las causas de los mismos además de posibles correcciones.
- Comprometer al cuerpo administrativo de la organización con la realización y puesta en marcha del proceso de auditorías.

- Suministrar constantemente información actualizada y consistente para poder liderar un proceso armónico.

- Proponer y trabajar por la optimización de todos los recursos involucrados en el proceso de auditoría.

- Evitar a toda costa la improvisación

Veamos el siguiente gráfico que nos resume los objetivos de la planeación de la auditoría de sistema.

Objetivos Planeación de la Auditoría

Ahora sí, entremos en materia y hablemos de la planeación de la auditoría de sistemas.

No hay un lineamiento específico que oriente el desarrollo de un proceso de auditoría de sistemas, pues cada proyecto es diferente y por ende debe manejarse con una estrategia diferente teniendo en cuenta el alcance de la misma, los riesgos y su dimensión.

La falta de planeación es el principal factor de los errores y retrasos, costos elevados y la baja calidad del proceso de auditoría; por ello se hace necesario una buena y dedicada planeación y que el auditor conozca la organización, el auditado y mientras más profundo este conocimiento, mucho mejor serán los resultados.

Aunque la experiencia ha mostrado que así los auditores conozcan mucho la organización auditada, este conocimiento no es suficiente en comparación con los empleados de la

organización que llevan largos períodos de tiempo en ésta; pero en sí, lo importante es tener el conocimiento necesario que le permita al auditor identificar todos los factores que puedan verse involucrados en la planeación de la auditoría.

Pero además de lo anterior, es necesario que el auditor tenga algún nivel de conocimiento de la razón o sector industria de la organización, del negocio en sí, de sus clientes y de todo aquello que se considere vaya a tener algún efecto sobre la información a evaluar.

En esta etapa de planeación, se deben enfocar los esfuerzos en la recopilación de la mayor cantidad de información posible sobre la Organización, para que esta le sirva para formular el plan de auditorías y obviamente para la ejecución posterior de la auditoría.

Algunos aspectos a tener en cuenta sobre el tipo de información a recolectar sobre la organización, podrían ser:

- Características Generales de la empresa (sector industria, qué hacen, organigrama).
- Recursos informáticos relacionados a cada área (descripción de Hardware y Software).
- Conceptos relacionados con la auditoría

Para lograr una efectiva planeación de la auditoría, es muy necesario obtener la información necesaria pero de manera selectiva, haciendo uso de mecanismos como las entrevistas, encuestas. Estos método son muy efectivos, pero todo depende de que tanta habilidad se posea para la acción de entrevistar y obtener la mayor cantidad de datos que de ésta se pueda obtener.

Una buena forma de tener éxito con las entrevistas, es planear el esquema de la entrevista, haciendo el formulario de esta.

Un ejemplo de este formulario o derrotero de preguntas para llevar a cabo la entrevista podría ser:

- ¿Cómo está constituida esta empresa? (Organigrama).
- ¿Con qué tipo de quipos cuenta la empresa (hardware), y cómo están distribuidos?
- ¿Con qué tipo de programas o aplicaciones (Software) cuenta la empresa?
- ¿Qué otro tipo de programas o aplicaciones la empresa ha identificado como que hacen falta por implementar?
- ¿Alguien del personal de la organización ha estado involucrado en el desarrollo de las aplicaciones de la organización? (si sí, cómo participó).

- ¿Las aplicaciones que están en uso en la organización, incluyen algunos conceptos de auditoría de sistemas? (si sí, cuáles).
- ¿En la empresa existe un Manual de Funciones?
- ¿Existe un Manual de Procedimientos?
- Existe un manual de usuario para las aplicaciones?
- ¿Hay un plan de Mantenimiento?
- ¿Hay algún procedimiento para el respaldo de la información (back-ups)?
- ¿Existen los Planes de Contingencias en la organización?

- ¿Esta área o departamento ha sido auditado de alguna manera? Interna o externamente? (Si sí, cada cuanto se ha hecho estas auditorías).
- ¿A usted le gustaría sugerir algo para el manejo del flujo de la información que se maneja actualmente?
- ¿Considera que alguno de los informes que se manejan hoy en el departamento son redundantes?
- ¿Con la información que usted cuenta hoy, puede tomar decisiones?
- ¿Usted considera que necesita acceder de manera más rápida a su propia Base de Datos o a sus archivos de información?
- ¿Algunos de los procesos que ejecuta se bloquean durante su ejecución?
- ¿Le gustan los reportes generados por el computador?

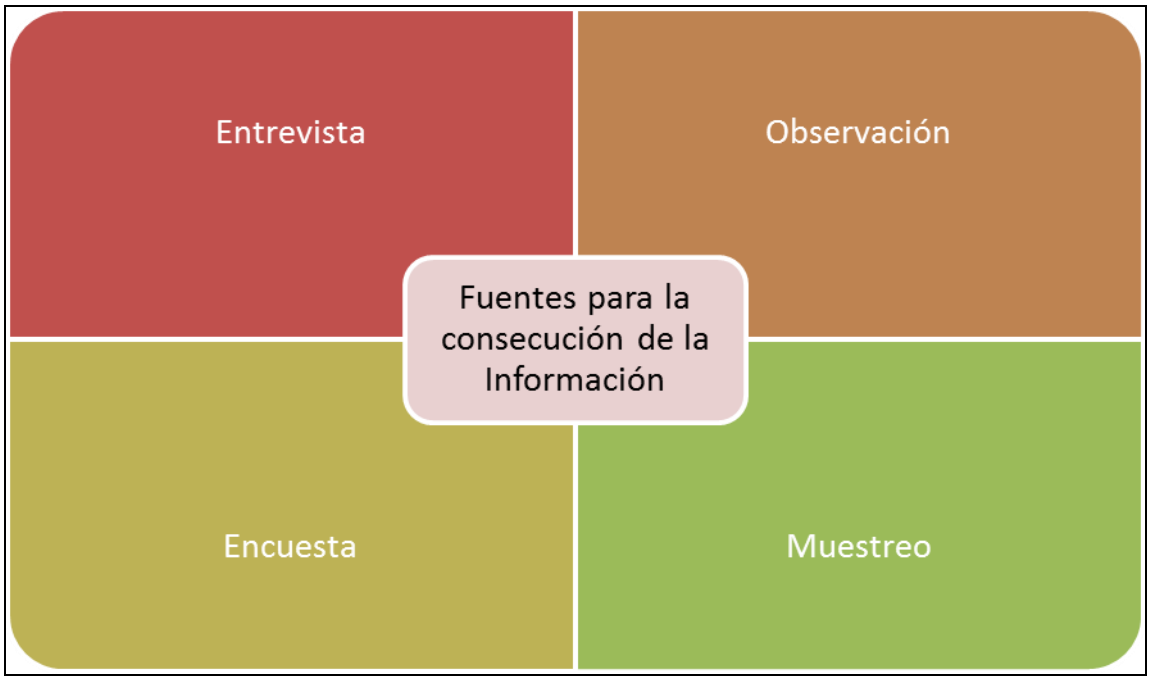
Es muy importante hacer las observaciones pertinentes que van de la mano con las tareas que realizan los empleados, esto con el fin de complementar la información recibida haciendo uso del mecanismo de la entrevista y además que esta información sirva como punto para la verificación de la misma con los hechos observados durante la auditoría.

Además, es necesario tener muy en cuenta que las observaciones deben hacerse muy discretamente para no entorpecer el curso normal de la actividad de la actividad en observación.

La encuesta es un método muy usado y puede aplicarse en un grupo grande, pero ésta debe ser muy bien planeada y diseñada, para que sus resultados si apunten a la consecución de la información esperada.

Teniendo en cuenta el tiempo del que se dispone para el trabajo con estas actividades de observación- entrevista, es necesario saber cuándo es posible hacerlas para toda la comunidad. Esto es, cuando hay suficiente tiempo para ello, de lo contrario es necesario hacer uso de la técnica estadística del muestreo, y puedan hacerse observaciones con una población aleatoria y que la información seleccionada para dicha muestra si arroje los suficientes datos como para hacer un análisis valioso.

La siguiente gráfica resume las técnicas que se pueden utilizar para encontrar la información necesaria para el proceso de auditoría:



Fuentes para la Información

EJERCICIO DE APRENDIZAJE:

Haciendo uso del gráfico "Fuentes para la información", escoger una de las 4 fuentes allí propuestas y diseñarla para un caso de auditoría particular que usted quiera.

4. UNIDAD 3 AUDITORÍAS DE SISTEMAS

OBJETIVO GENERAL

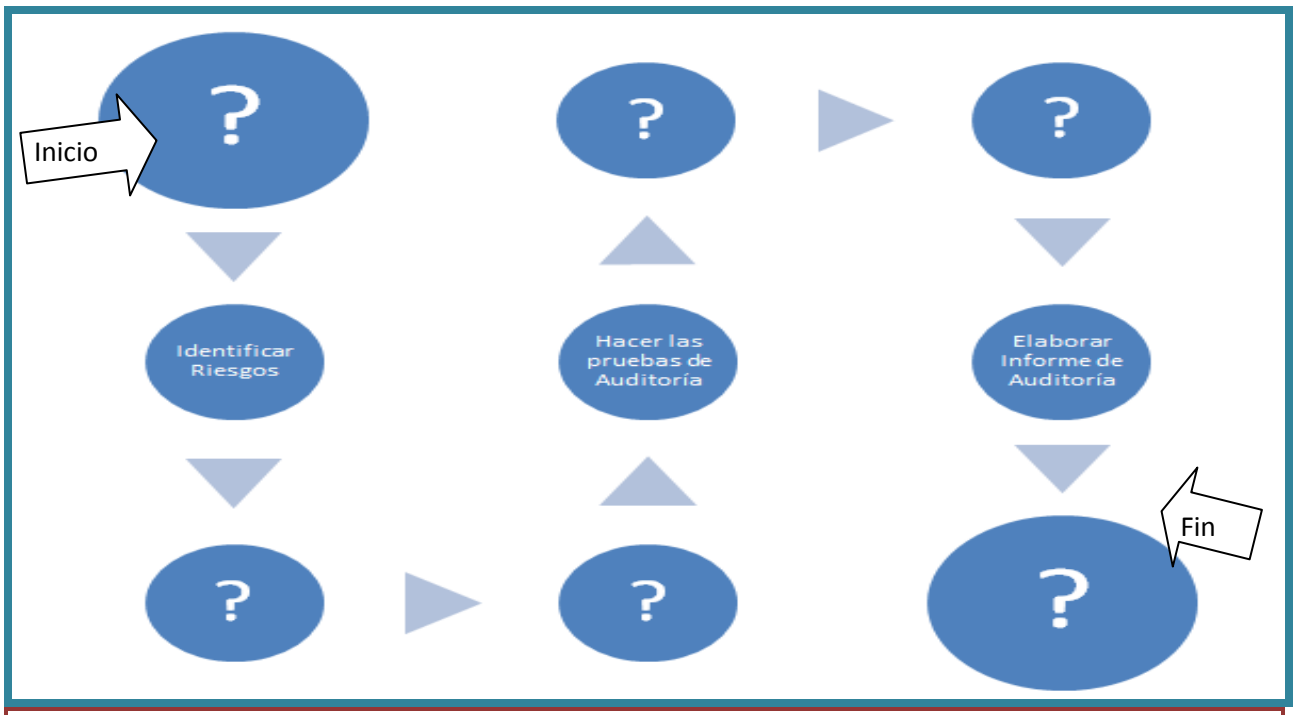
Evaluar las directrices para una auditoría de sistemas, además de su aplicabilidad en una organización

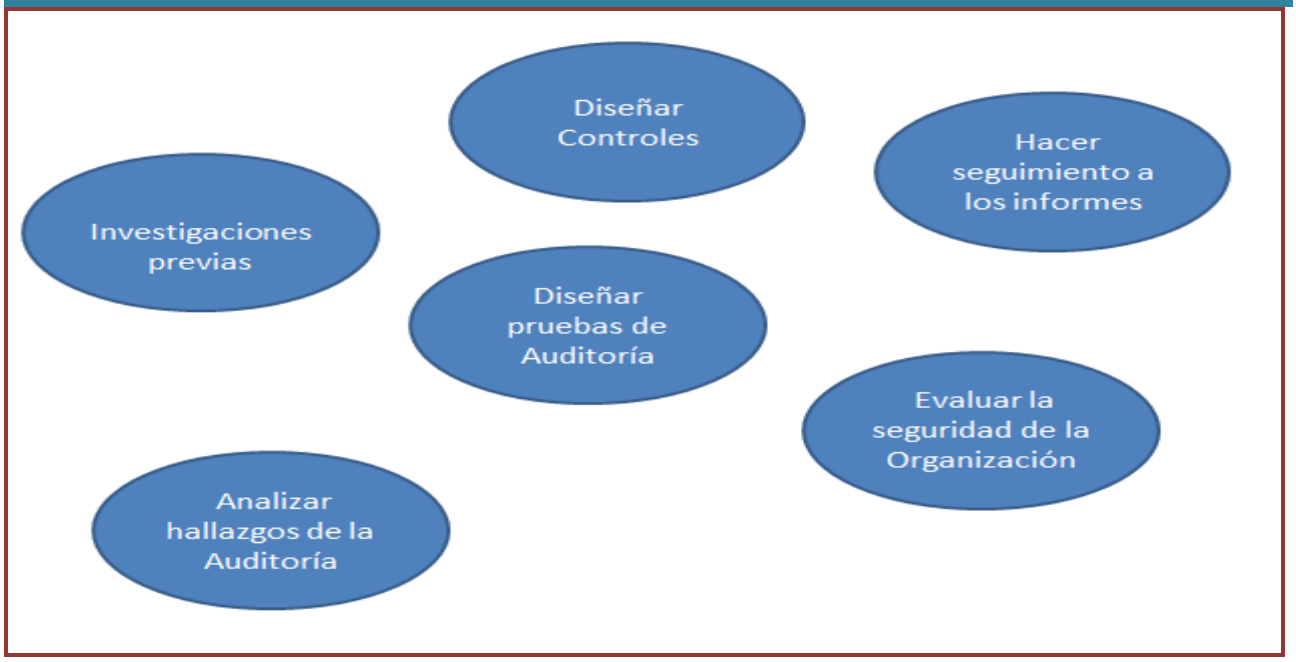
OBJETIVOS ESPECÍFICOS

- Establecer las pautas para la realización de una auditoría de sistemas.
- Analizar algunos ejemplos de auditorías de sistemas como medio para ver la aplicación de la teoría de auditorías en el campo de la informática.

Prueba Inicial

Complete los pasos con el símbolo de interrogante (¿) siguiendo el orden lógico que usted creería son las fases (recuadro en rojo), para desarrollar una auditoría.


Inicio
?
?
?
Identificar Riesgos
Hacer las pruebas de Auditoría
Elaborar Informe de Auditoría
?
?
?
Fin

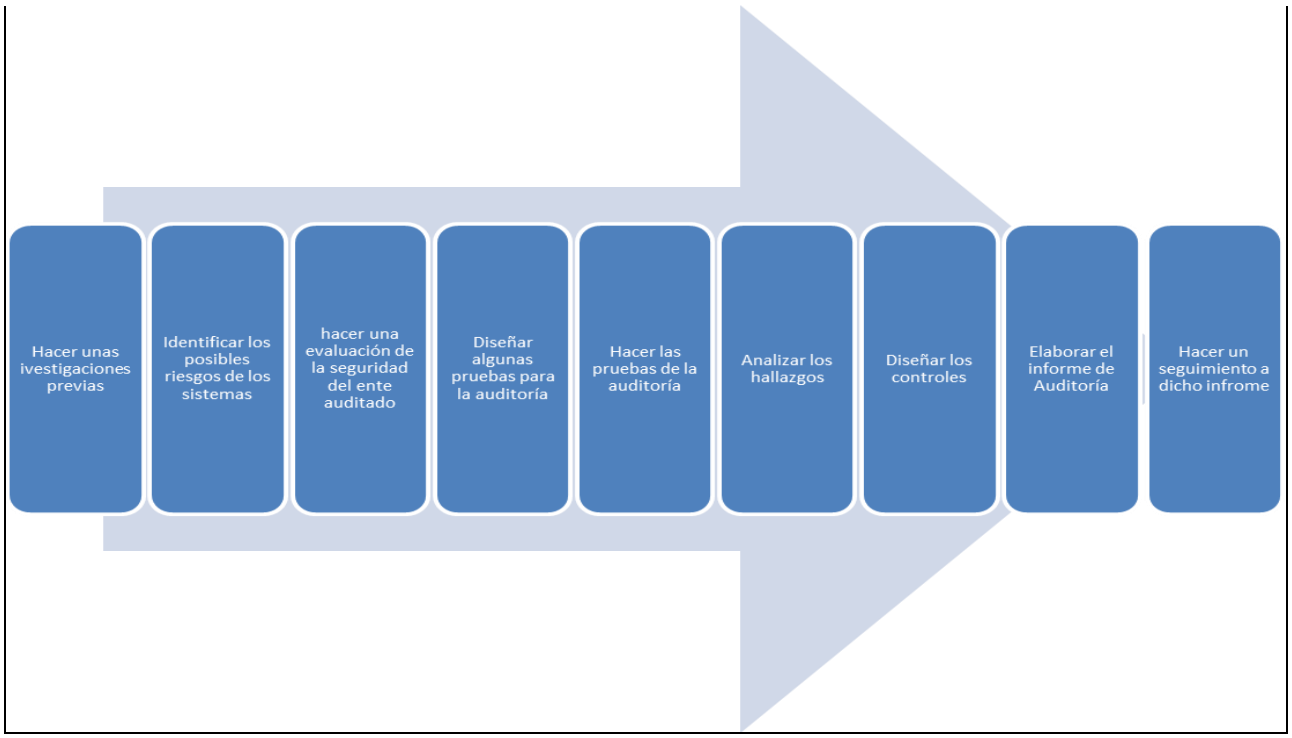

Diseñar Controles
Hacer seguimiento a los informes
Investigaciones previas
Diseñar pruebas de Auditoría
Evaluar la seguridad de la Organización
Analizar hallazgos de la Auditoría

4.1. Fases de la Auditoría de Sistemas Y su Seguimiento

Acerquémonos a las fases de una auditoría de sistemas en un caso real, viendo el siguiente video: http://www.youtube.com/watch?v=0V0EsVs0-C4&feature=related

Video Intro Unidad3

En esta unida ya entraremos un poco más en materia, veremos cómo realizar entonces una auditoría de Sistemas. Veamos entonces las fases o pasos que se deben tener en cuenta para la realización de una auditoría:



Fases para la Auditoría de Sistemas

Para comenzar es muy necesario que conozcan los siguientes aspectos previamente:

1. Conocer de manera general la organización, esto en aspectos como:

a. Área de sistemas
b. Organigrama de la Organización
c. Equipos de la Organización
d. Sistemas de la Organización
e. Sistema de Redes y Telecomunicación

2. Ahora para la investigación previa, realice las siguientes actividades:

a. Entrevistas a los auditados
b. Visita a las instalaciones de la organización auditada
c. Entrevistas informales a las personas involucradas con el sistema a auditar.
d. Revisar todo tipo de documentos facilitados por la organización
e. Revisar reportes o informes de auditorías que se hayan realizado en previas auditorías.
f. Analizar el sistema o los sistemas de control interno de la organización.

3. Algunos de los documentos que se deben solicitar a la organización para dicha actividad preliminar son:

- Lista de aplicaciones de la organización
- Lista de los empleados de la organización (con estado activo o despedidos durante el tiempo que ha transcurrido desde la última auditoría hasta esta)
- Información de los usuarios de los sistemas y sus respectivos privilegios
- Lista de chequeo o revisiones del sistema
- Políticas de seguridad de los sistemas de la organización
- Políticas de seguridad de la Organización.
- Documentos de configuración de los sistemas (con los respectivos cambios hechos)
- Lista de los Roles de los administradores del sistema y la seguridad de los mismos.
- Planes de cualificación y capacitación del personal
- Los reportes de las auditorías anteriores

4. Para comenzar el trabajo de estudio de la auditoría de sistemas, veamos este proceso organizado por partes así:

5. Instalación y configuración de los equipos

- Políticas para la instalación y la configuración inicial.
- Configuración de los servicios como.
- Configuración de los parámetros de seguridad.
- Los sistemas de archivos.
- Las particiones y sus configuraciones.
- Los programas (SW) instalado.

6. Seguridad Física

- Acceso del personal al departamento de sistemas y a la sala de telecomunicaciones (closet de los servidores).
- Señalización.
- Instalación del sistema eléctrico.
- Estado UPS
- Almacenamiento de cintas, discos y documentación
- Entorno del closet de telecomunicaciones (temperatura, humedad, ventilación).
- Ubicación de equipos.
- Aseo.

7. Seguridad Lógica

- Control de acceso a objetos del sistema.
- Archivos con permisos especiales.
- Mecanismos de identificación y autenticación.
- Administración de usuarios.
- Administración de cuentas.
- Perfiles de los usuario.
- Control de usuarios especiales.
- Manejo de cuentas especiales.
- Proceso de encendido /apagado y de inicio y cierre de sesión.
- Proceso de arranque del sistema.
- Cifrado de datos
- Acceso remoto.

8. Documentación del Sistema

- Políticas y estándares de los procesos relacionados con el sistema a auditar
- Políticas de seguridad de la organización.
- Manuales del sistema a auditar.
- Manuales de procedimientos.
- Manuales de usuario.
- Manuales de funciones.
- Documentación de la instalación y configuración inicial del sistema a auditar.
- Póliza de seguros para los sistemas y los equipos.

9. Mantenimiento y soporte

- Soporte por parte del proveedor.
- Control de la realización de tareas de mantenimiento.
- Planes de mantenimiento lógico y físico.
- Contratación de mantenimiento y soporte.
- Actualizaciones realizadas a los equipos (HW).
- Actualizaciones realizadas.

10. Aspectos administrativos

- Estructura de la Organización (organigrama).
- Definición de roles y funciones.

- Selección y contratación de personal
- Capacitación y entrenamiento.
- Ambiente laboral.

11. Monitoreo y Auditoría

- Evaluación de la función de auditoría interna (si se cuenta con ésta) o la externa.
- Procedimientos de auditoría realizados con relación a este sistema a auditar.
- Existencia y utilización de herramientas de monitoreo y auditoría.
- Procedimientos de monitoreo.
- Reportes de monitoreo y auditoría.

12. Planes de respaldo y recuperación (Planes de Contingencia)

- Que exista un plan de contingencia.
- Conocimiento y divulgación del plan de contingencias.
- Pruebas y ajustes al plan de contingencias.
- Planes de respaldo
- Elaboración y gestión de copias de seguridad (Backups)

13. Administración e implementación de la seguridad

- Función encargada de la administración de la seguridad.
- Roles y responsabilidades.
- Políticas y estándares.
- Entrenamiento y capacitación en seguridad.
- Personal de asesoría
- Procedimientos de administración de la seguridad.
- Almacenamiento
- Documentación.

EL SEGUIMIENTO DE LA AUDITORÍA DE SISTEMAS:

En consiste el seguimiento a la auditoría de sistemas?, Este pretende valor dos aspectos claves:

1. La calidad del funcionamiento del sistema, es decir, evaluar características como su aplicabilidad, si los sistemas están completos y son congruentes con sus competencias, si brindan seguridad.

2. La calidad de la Gestión de la Organización, es decir, medir su eficiencia, eficacia, si la información que proveen es confiable y oportuna, si hay respaldo y legalidad con su patrimonio y sus objetivos.

Algunas generalidades o preguntas claves a tener en cuenta en el Seguimiento son:

- Cómo
- Qué
- Para qué
- Tipos
- Quién debe hacerlo
- Por qué

Veamos el siguiente gráfico que nos recuerda qué preguntarnos en el seguimiento.

Preguntas para el seguimiento

El seguimiento además también debe hacerse al programa de auditorías, donde se evalúen aspectos como:

- La Aptitud de los auditores para seguir el programa de auditorías. No se puede olvidar que una mala actitud del auditor puede llevar a que la evaluación se vea viciada, o sus resultados sean alterados de una u otra manera.

- Que gracias a la Organización y el auditor, los cronogramas y planes de auditoría se estén siguiendo a tiempo de acuerdo a la planeación establecida previamente a la ejecución de las auditorías.

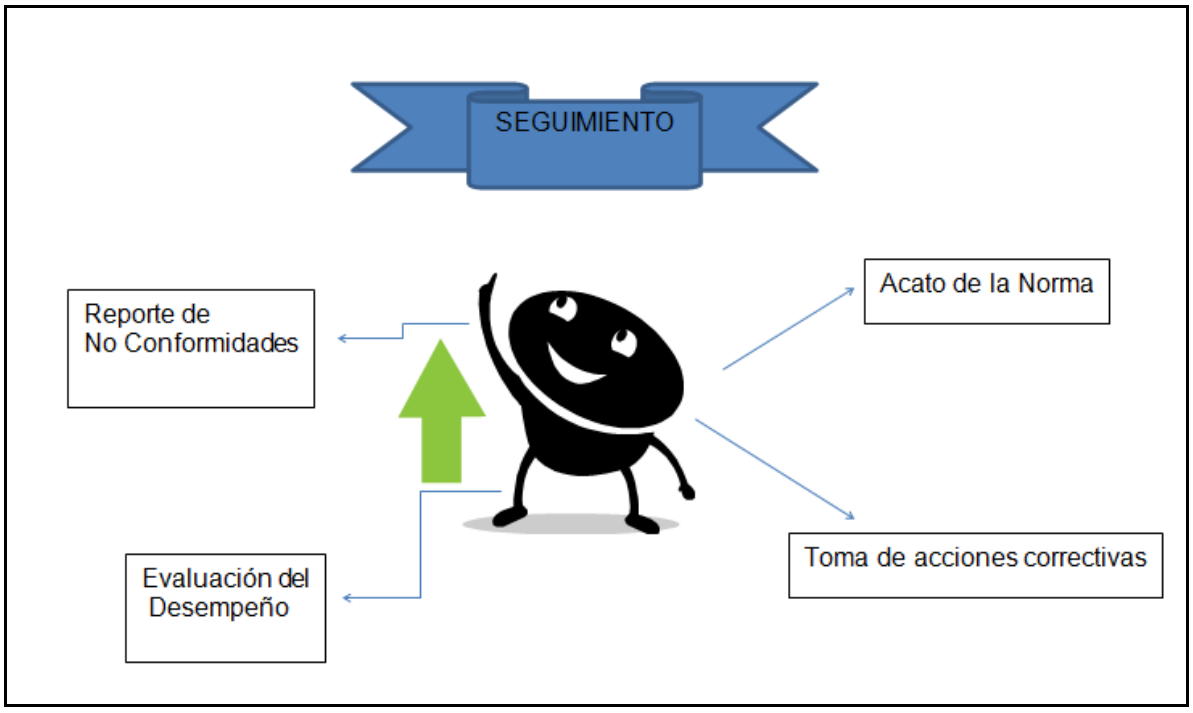
- Que se esté realizando una retroalimentación por parte de auditores y auditados para ir analizando los resultados de dicha evaluación.

- Que se estén llevando a cabo los registros de la auditoría.

- Que haya coherencia en las acciones tomadas por el auditor y otros auditores previos (si existiere el caso de auditorías previas).

- Que se evidencie en el auditor prácticas de auditoría nuevas o alternativas.

Las Normas Generales que se deben tener en cuenta para el seguimiento de las auditorías se resumen en el siguiente gráfico.



Normas para el seguimiento

EJERCICIO DE APRENDIZAJE:

1. Explique en sus palabras, por qué debe hacerse "el seguimiento" a los informes de auditorías?
2. ¿En cuáles casos consideras no es necesario hacer seguimiento?

4.2. Casos para analizar el porqué de las auditorías en los sistemas

A continuación vamos a leer un artículo tomado del portal web Auditoría de Sistemas, en: http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/

"**EL ENEMIGO EN CASA: INFRACCIONES INFORMÁTICAS DE LOS TRABAJADORES**

La proliferación de las nuevas tecnologías en la empresa conlleva también la proliferación de nuevos peligros. Ya no son sólo los ataques y sabotajes informáticos desde el exterior, sino las infracciones desde dentro, las producidas por los propios empleados, y contra las que las organizaciones son, al parecer, más vulnerables. Hace poco más de un mes, la firma Landwell de Abogados y Asesores Fiscales, perteneciente a PricewaterhouseCoopers, presentaba un excelente estudio titulado Actos desleales de trabajadores usando sistemas informáticos, el cual merece la pena conocer con algo de detalle en estas páginas.

El estudio se ha elaborado a partir del análisis de informes, sentencias, autos y procedimientos judiciales de 393 casos reales sufridos por empresas españolas y protagonizados por trabajadores en plantilla, durante el trienio 2001-2003; y se ha completado con entrevistas personales con los responsables de las compañías afectadas.

Para empezar, el informe reconoce que se desconoce el nivel de incidencia en el conjunto total de las empresas españolas, ya que una gran parte de las empresas afectadas por este tipo de acciones prefieren llegar a un acuerdo amistoso y no divulgar los hechos. Las infracciones más habituales que han sido detectadas son así sistematizadas en el estudio:

- Creación de empresa paralela, utilizando activos inmateriales de la empresa. Consiste en la explotación en una empresa de nueva creación, de la propiedad intelectual, la propiedad industrial o el know how de la empresa en la que el trabajador trabaja. Generalmente, el

trabajador constituye la nueva compañía antes de solicitar la baja voluntaria y realiza un proceso de trasvase de información mediante soportes informáticos o a través de Internet. Es posible que el trabajador actúe aliado con otros compañeros de la empresa.

- Daños informáticos y uso abusivo de recursos informáticos. Los daños informáticos se producen generalmente como respuesta a un conflicto laboral o a un despido que el trabajador considera injusto. Consisten en la destrucción, alteración o inutilización de los datos, programas o cualquier otro activo inmaterial albergado en redes, soportes o sistemas informáticos de la empresa. Los casos más habituales son los virus informáticos, el sabotaje y las bombas lógicas, programadas para que tengan efecto unos meses después de la baja del trabajador.

- También es habitual el uso abusivo de recursos informáticos, especialmente el acceso a Internet. Información confidencial y datos personales. Consiste en el acceso no autorizado y en la posterior revelación a terceros, generalmente competidores o clientes, de información confidencial de la empresa. En algunas ocasiones, la revelación la realizan trabajadores que tienen un acceso legítimo, pero con obligación de reserva, a la información posteriormente divulgada. En este capítulo también se contempla la cesión no autorizada a terceros de datos personales de trabajadores y clientes. Amenazas, injurias y calumnias. El medio utilizado habitualmente es el correo electrónico corporativo, aunque también se han utilizado cuentas anónimas, e incluso se ha suplantado la identidad de otro trabajador de la misma empresa. En el caso de las amenazas, se busca un beneficio material o inmaterial para el trabajador. Si el beneficio no se produce, el trabajador llevará a cabo la conducta anunciada en el mensaje amenazador. En el caso de las injurias y las calumnias, se busca desacreditar a la empresa, o a alguno de sus directivos.

- También se han producido insultos a clientes habituales o a clientes potenciales de la empresa con el que el trabajador tenía algún conflicto. Infracción propiedad intelectual e introducción de obras de la empresa en redes P2P. Consiste en la copia de activos inmateriales de la empresa, especialmente obras protegidas por la propiedad intelectual, con el fin de cederlas posteriormente a terceros.

En los últimos dos años se han dado casos de difusión a través de Internet, mediante el uso de redes de intercambio de ficheros (peer to peer). De esta manera, una multitud de usuarios acceden de forma gratuita a programas de ordenador desprotegidos, información o contenidos multimedia. Intercambio de obras de terceros a través de redes P2P.

Este es el caso más habitual y se detecta generalmente en el curso de una auditoría de seguridad informática, mediante el análisis del caudal de datos transferido por los trabajadores a través de la

red corporativa. En algunas ocasiones, se ha detectado directamente la instalación del programa P2P o el uso de puertos típicos para el acceso a redes P2P. Este caso es especialmente grave, ya que la empresa se convierte en proveedora directa de copias no autorizadas de música, películas y programas de ordenador. Infracción de derechos de propiedad industrial.

- El caso más habitual ha sido la infracción de marcas de la empresa mediante el registro del nombre de dominio por parte del trabajador. En algunos casos, se ha creado una página web con contenidos ofensivos para conseguir un mayor efecto nocivo para la empresa o para obtener una suma de dinero por la transferencia.

Ante la aparición de esta clase de situaciones, ¿cuál ha sido la estrategia de respuesta de las empresas?

El informe de Landwell nos dice que la mayoría de las empresas prefieren encomendar la investigación de los posibles actos desleales de un trabajador a un equipo interno, generalmente formado por miembros del departamento de RRHH y del departamento de sistemas.

Sólo un 22 por ciento (22%) de las empresas que sospechan de un empleado deciden externalizar la investigación. El tipo de investigación depende de la intención de la empresa de llegar a un acuerdo o plantear una reclamación judicial.

Cuando se toma la decisión de llevar la infracción a los tribunales, la obtención de las evidencias electrónicas se encarga a un tercero, con el fin de conseguir mayor objetividad y valor probatorio. El procedimiento de recopilación de las evidencias debe respetar los derechos del trabajador para que sea válido judicialmente. Una investigación se inicia a partir de las sospechas e indicios generados por la propia conducta del trabajador, por un consumo de recursos poco usual o por el descubrimiento de los efectos de la infracción.

No obstante, Sólo el 26 por ciento de las infracciones detectadas acaban en los tribunales. El resto de las infracciones son objeto de un acuerdo privado o de una sesión finalizada con avenencia en un organismo de mediación y conciliación laboral. En general, las empresas prefieren solucionar sus conflictos de forma privada y ello incide en la forma de investigar y tratar las posibles infracciones de sus trabajadores.

Ahora bien, si los daños producidos están previstos en la cobertura de un seguro, es muy probable que la empresa deba plantear una reclamación judicial para poder solicitar la correspondiente compensación económica".

Con los anteriores casos que nos presentaron en el anterior artículo, debemos recordar que toda la información de la empresa es muy importante y hoy en día es parte de los activos de la organización, y así mismo debe invertirse en la protección de la misma, y esto es bien logrado con unos procesos de auditoría de sistemas.

Estas auditorías entran en especial funcionamiento en el momento en el que hay grandes cambios fuertes en los sistemas de la organización.

Las organizaciones a través de sus auditorías internas, pueden ir evaluando sus procesos y la seguridad de sus sistemas informáticos.

Así mismo la organización debe acudir a las auditorías externas cuando se percibe debilidad en la ejecución de los procesos de la misma. Algunos ítems que nos podrían llamar la atención para aplicar una auditoría externa, de acuerdo al portal de Auditoría de Sistemas en: http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/ son:

"**SÍNTOMAS DE DESCOORDINACIÓN Y DESORGANIZACIÓN:**

No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía. Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.

SÍNTOMAS DE MALA IMAGEN E INSATISFACCIÓN DE LOS USUARIOS:

No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.

No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.

No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.

SÍNTOMAS DE DEBILIDADES ECONÓMICO-FINANCIERO

Incremento desmesurado de costes.

Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).

Desviaciones Presupuestarias significativas.

Costes y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).

SÍNTOMAS DE INSEGURIDAD: EVALUACIÓN DE NIVEL DE RIESGOS

Seguridad Lógica

Seguridad Física

Confidencialidad: [Los datos son propiedad inicialmente de la organización que los genera. Los datos de personal son especialmente confidenciales]

CENTRO DE PROCESO DE DATOS FUERA DE CONTROL

Si tal situación llegara a percibirse, sería prácticamente inútil la auditoria. Esa es la razón por la cual, en este caso, el síntoma debe ser sustituido por el mínimo indicio”.

EJERCICIO DE APRENDIZAJE: Realice un mapa conceptual donde explique los casos donde debe considerarse una auditoría externa.

Ahora veamos un ejemplo de un caso de estudio (Auditoría de Sistemas) realizada por un grupo de estudiantes de la Universidad de Caldas, a una empresa de Lácteos, en el proceso de Administración de datos. (En: http://ingenieria.ucaldas.edu.co/auditoria/index.php/Grupo_7).

CHAUDITORIA CONSULTORES S.A.				
Empresa a Auditar	**Objetivo de Control**	**Fecha Auditoria**		
NATURA LACTEOS LTDA.	**PO3 Determinar la Dirección Tecnológica**	20	05	09
Auditores	Andrés Felipe Franco M. Mauricio Orozco Buitrago	Grupo 7		
Responsables Auditados	Edwar Augusto Jaramillo Soto Maricela Zuloaga Sandra Milena Hernández Patiño	Grupo 2		
El propósito de está auditoria es *determinar la dirección tecnológica* de la empresa **Natura Lácteos** para así permitir dar soporte tecnológico adecuado para una empresa de esta índole. Se busca los sistemas del negocio, la arquitectura de la información y los estándares tecnológicos con que cuenta **Natura Lácteos.** Para detectar el incumplimiento de los estándares tecnológicos, desviaciones con respecto al plan de infraestructura tecnológica.				

Ejemplo auditoría

Se determina el propósito u Objetivo de la Auditoría como carta de navegación de todo el proceso de auditoría

ORIGEN DE LA AUDITORIA.

La presente auditoria se realiza en cumplimiento de la solicitud que la empresa Natura Lácteos Ltda. Ha hecho a Chauditoria Consultores S.A, en su afán de detectar posibles síntomas de debilidad y de evaluar la eficiencia y efectividad en sus procesos de administración de datos.

1. GUÍA AUDITORA

Objetivos de Control

- Planificar la infraestructura tecnológica.
- Supervisar las futuras tendencias y regulaciones.
- Tener planes de contingencia de la infraestructura tecnológica.
- Tener planes de adquisiciones de hardware y software.
- Poseer estándares tecnológicos.

Obtención de Conocimiento
Recurso Humano a consultar
Gerente General Jefe del Departamento de Finanzas Gerencia de Sistemas

Información a conocer

- Políticas y procedimientos relacionados con planificación y el seguimiento de la infraestructura tecnológica.
- Tareas y responsabilidades de planificación de la dirección.
- Objetivos a largo y corto plazo de Natura Lácteos.
- Objetivos a largo y corto plazo de la tecnología de la información.
- Plan de adquisición de hardware y software de Natura Lácteos.
- Plan de infraestructura tecnológica.
- Informes de estado y actas de reuniones del comité de planificación.

2. Aspectos a Evaluar

Evaluación de los controles, considerando si:

Existe un proceso para la creación y la actualización regular del plan de infraestructura tecnológica para confirmar que los cambios propuestos están siendo examinados primero para evaluar los costos y riesgos inherentes, y que la aprobación de la Dirección se obtiene antes de realizar cualquier cambio en el plan.
El plan de infraestructura tecnológica está siendo comparado con los planes a largo y corto plazo de la tecnología de la información.

Existe un proceso para la evaluación de la situación tecnológica actual de la organización para asegurar que abarca aspectos tales como la arquitectura de sistemas, la dirección tecnológica y las estrategias de migración.

La política y procedimientos de los servicios de información aseguran la consideración de la necesidad de evaluar y realizan un seguimiento de las tendencias y condiciones regulatorias tecnológicas presentes y futuras, y si éstas se tienen en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.

Se planifican el impacto logístico y ambiental de las adquisiciones tecnológicas.

Las políticas y procedimientos de los servicios de información aseguran que se considera la necesidad de evaluar sistemáticamente el plan tecnológico con respecto a contingencias (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).

La dirección de los servicios de información evalúa tecnologías de vanguardia, e incorpora tecnologías apropiadas a la infraestructura de los servicios de información actual.

Los planes de adquisición de hardware y software suelen satisfacer las necesidades identificadas en el plan de infraestructura tecnológica y si éstos se aprueban apropiadamente.

Se encuentran establecidos los estándares de la tecnología para los componentes tecnológicos descritos en el plan de infraestructura tecnológica.

Evaluación de la suficiencia, probando que:

La dirección de los servicios de información comprende y utiliza el plan de infraestructura tecnológica.

Se han realizado cambios en el plan de infraestructura tecnológica para identificar los costos y riesgos inherentes, y que dichos cambios reflejan las modificaciones a los planes a largo y corto plazo de la tecnología de la información.

La dirección de los servicios de información comprende el proceso de seguimiento y evaluación de las nuevas tecnologías e incorpora tecnologías apropiadas a la infraestructura de los servicios de información actual.

La dirección de los servicios de información comprende el proceso de evaluar sistemáticamente el plan tecnológico en cuanto a contingencias (por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura).

Existe un espacio adecuado en los servicios de información adecuado para alojar el hardware y software actualmente instalado, así como nuevo hardware y software adquirido según el plan de adquisiciones actual aprobado.

El plan de adquisición de hardware y software cumple con los planes a largo y corto plazo de la tecnología de la información, reflejando las necesidades identificadas en el plan de infraestructura tecnológica.
El plan de infraestructura tecnológica dirige la utilización de la tecnología actual y futura.

Se cumple con los estándares de la tecnología y que éstos son agregados e incorporados como parte del proceso de desarrollo.

El acceso permitido es consistente con los niveles de seguridad definidos en las políticas y procedimientos de los servicios de información, y se ha obtenido la autorización apropiada para el acceso.

Evaluación del riesgo
Llevando a cabo:

Mediciones ("Benchmarking") de la planificación de la infraestructura tecnológica en relación con organizaciones similares o estándares internacionales y buenas prácticas reconocidas en la industria del sector.

Una revisión detallada del diccionario de datos para verificar que está completo en lo referente a elementos clave.

Una revisión detallada de los niveles de seguridad definidos para datos confidenciales.

Identificando:
Inconsistencias en el modelo de la arquitectura de la información y en el modelo y el diccionario de datos corporativo, en los sistemas de información asociados y en los planes a largo y corto plazo de la tecnología de la información. Elementos del diccionario de datos y reglas de sintaxis de datos obsoletos.

Contingencias que no han sido consideradas en el plan de infraestructura tecnológica.
Planes de adquisición de hardware y software de la tecnología de la información que no reflejan las necesidades del plan de infraestructura tecnológica.

Estándares de la tecnología que no son consistentes con el plan de infraestructura tecnológica o con los planes de adquisición de hardware y software de la tecnología de la información.
Un plan de infraestructura tecnológica o planes de adquisición de hardware y software de la tecnología de la información que no son consistentes con los estándares de la tecnología. Elementos clave omitidos en el diccionario de datos.

CHAUDITORIA CONSULTORES S.A.				
Empresa a Auditar	Objetivo de Control	Fecha Auditoria		
NATURA LACTEOS LTDA.	AI1 Identificar Soluciones Automatizadas	20	05	09
Auditores	Andrés Felipe Franco M. Mauricio Orozco Buitrago	Grupo 7		
Responsables Auditados	Edwar Augusto Jaramillo Soto Maricela Zuloaga Sandra Milena Hernández Patiño	Grupo 2		

Ejemplo auditoría 1

ORIGEN DE LA AUDITORIA.

La presente auditoria se realiza en cumplimiento de la solicitud que la empresa Natura Lácteos Ltda. Ha hecho a Chauditoria Consultores S.A, en su afán de detectar posibles síntomas de debilidad y de evaluar la eficiencia y efectividad en sus procesos de administración de datos.

1. **GUÍA AUDITORA**

Objetivos de Control

- Definir los requerimientos de la información.
- Formular las acciones alternativas.
- Formular las estrategias de Adquisición.
- Saber cuáles son el requerimiento de servicios de terceros (mantenimiento de impresoras).
- Estudiar de Viabilidad Tecnológica.
- Estudiar de Viabilidad Económica.
- Informe de Análisis de los riesgos.
- Controles de Seguridad Eficaces en costo.
- Ergonomía. • Selección del Software del Sistema.
- Control de Abastecimiento.
- Aceptación de Instalaciones.
- Aceptación de la Tecnología.

Obtención de Conocimiento
Recurso Humano a consultar:
Gerente de sistemas Jefe área de seguridad informática Jefe área de proyectos

Información a conocer:

- Políticas y procedimientos relacionados con el ciclo de vida de desarrollo de los sistemas.
- Objetivos y planes a corto y largo plazo de la tecnología de la información.
- Documentación seleccionada del proyecto, incluyendo definición de requerimiento, análisis de alternativas, estudios de viabilidad tecnológica,
- Estudios de viabilidad económica, análisis de modelos de datos de la empresa y arquitectura de la información, análisis de los riesgos, estudios de economía sobre control y seguridad interna, análisis de pistas de auditoría, estudios ergonómicos, y planes de aceptación y resultados de pruebas de instalaciones y tecnología específica.

Aspectos a Evaluar
Evaluación de los controles, considerando si:

- Existen políticas y procedimientos que requieren que:
- Los requerimientos de los usuarios satisfechos por el sistema existente o a ser satisfechos por el nuevo sistema propuesto o modificado están claramente definidos antes de la aprobación de cualquier proyecto de desarrollo, implementación o modificación.
- Los requerimientos de los usuarios son revisados y aprobados por escrito antes de la aprobación de cualquier proyecto de desarrollo, implementación o modificación.
- Los requerimientos operativos y funcionales de la solución son satisfechos incluyendo rendimiento, seguridad, confiabilidad, compatibilidad y legislación.
- Las soluciones alternativas a los requerimientos de los usuarios son estudiadas y se estudian y analizan antes de seleccionar una u otra solución de software.
- Se lleva a cabo la identificación de paquetes de software comercial que satisfacen los requerimientos para un proyecto específico de desarrollo o modificación antes de tomar la decisión final.

- Las alternativas de desarrollo de productos de software están claramente definidas en términos de practicidad, internamente desarrollados, a través del contacto o mejora del software existente o una combinación de todos los anteriores.

- Se analiza y aprueba un estudio de viabilidad técnica para cada alternativa con el fin de satisfacer los requerimientos del usuario establecidos para el desarrollo de un proyecto de los sistemas tanto nuevos como modificados.

- En cada proyecto de desarrollo, modificación o implementación de los sistemas, se lleva a cabo un análisis de los costos y beneficios asociados con cada alternativa considerada para satisfacer los requerimientos del usuario.

- Se prepara, analiza y aprueba un estudio de viabilidad económica antes de tomar la decisión respecto a desarrollar o modificar un proyecto de los sistemas tanto nuevos como modificados.

- Se presta atención al modelo de datos de la empresa mientras se identifica y analiza la viabilidad de las soluciones.

- En cada proyecto de desarrollo, implementación o modificación de los sistemas propuestos, se prepara y documenta un análisis de las amenazas a la seguridad, de las debilidades y los impactos potenciales y las medidas factibles de seguridad y control interno para reducir o eliminar el riesgo identificado.

- Los costos y los beneficios de seguridad son examinados cuidadosamente para garantizar que los costos de los controles no exceden los beneficios.

- Se obtiene una aprobación formal del estudio de los costos y beneficios por parte de la dirección.

- Se requieren controles y pistas de auditoría apropiados para ser aplicados en todos los sistemas modificados o nuevos propuestos durante la fase de diseño del proyecto.

- Las pistas de auditoría y los controles dan la posibilidad de proteger a los usuarios contra la identificación o mal uso de su identidad por parte de otros usuarios (ej., ofreciendo anonimato, pseudónimos, ausencia de vínculos y confidencialidad).

- Cada proyecto de desarrollo, implementación o modificación de los sistemas propuesto presta atención a los problemas ergonómicos asociados con la introducción de los sistemas automatizados.

- La dirección de los servicios de información identifica todos los programas de software de los sistemas potenciales que satisfacen sus requerimientos. _ Los productos son revisados y probados antes de ser adquiridos y utilizados.

- En caso de requerirse la compra de productos de software cumple con las políticas de adquisición de la organización definiendo el marco de referencia para la solicitud de propuesta, la selección del proveedor de software y la negociación del contrato.

- Para el software con licencia adquirido a terceros, los proveedores cuenten con procedimientos apropiados para validar, proteger y mantener los derechos de integridad de los productos de software.

- Los servicios de programación se justifican a través de un requerimiento de servicios escrito por parte de un miembro designado de los servicios de información.

- Se acuerda en el contrato con el proveedor un plan de aceptación de las instalaciones y que dicho plan defina los procedimientos y criterios de aceptación.

- Se acuerda en el contrato con los proveedores un plan de aceptación para tecnología específica, y que dicho plan defina los procedimientos y criterios de aceptación.

- En caso de adquisición de servicios de programación adquiridos a terceros se justifica a través de una solicitud por escrito de los servicios por parte de un miembro designado de los servicios de información.

- Los productos finales de los servicios de programación contratados se han terminado, son revisados y probados de acuerdo con los estándares establecidos por el grupo encargado de asegurar la calidad de los servicios de información y otras partes interesadas antes de pagar por el trabajo realizado y aprobar el producto final.

- Se lleva a cabo un análisis de los riesgos en línea con el marco de referencia general de evaluación de los riesgos.

- Existen los mecanismos para asignar o mantener los atributos de seguridad para la exportación e importación de datos, y para interpretarlos correctamente.

- La dirección ha desarrollado e implementado un enfoque de adquisición central, que describe un conjunto común de procedimientos y estándares que deben ser seguidos, en

la adquisición de servicios de hardware, software y servicios de la tecnología de la información.

- Los contratos estipulan que el software, la documentación y las entregas están sujetos a pruebas y revisiones antes de ser aceptados.

- Las pruebas incluidas en las especificaciones de desarrollo consisten en pruebas de sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de rendimiento, pruebas de regresión, pruebas de aceptación del usuario, y finalmente, pruebas piloto del sistema total para evitar cualquier fallo inesperado del sistema.

- Las pruebas de aceptación de las instalaciones son llevadas a cabo para garantizar que éstas y el entorno, satisfacen los requerimientos especificados.

- Las pruebas de aceptación de la tecnología específica deberían incluir inspección, pruebas de funcionalidad y carga de trabajo.

Evaluación de la suficiencia, probando que:

- Los requerimientos de los usuarios satisfechos por el sistema existente y a ser satisfechos por el sistema nuevo o modificado han sido claramente definidos, revisados y aprobados por escrito por parte del usuario antes del desarrollo, implementación o modificación del proyecto.

- Los requerimientos de las soluciones funcionales se satisfacen incluyendo rendimiento, seguridad, confiabilidad, compatibilidad y legislación.

- Todas las debilidades y deficiencias de procesamiento en el sistema existente son identificadas y tomadas en cuenta y resueltas completamente por el sistema nuevo o el modificado.

- Los cursos alternativos que satisfacen los requerimientos de los usuarios, establecidos para un sistema nuevo o modificado, son analizados apropiadamente.

- Los paquetes de software comercial que satisfacen las necesidades de un proyecto particular de desarrollo o modificación de los sistemas son identificados y considerados apropiadamente.

- Todos los costos y beneficios identificados asociados con cada alternativa han sido soportados apropiadamente e incluidos como parte del estudio de viabilidad económica.

- Se ha prestado atención al modelo de datos de la arquitectura de la información y de la empresa al identificar y analizar su viabilidad.

- El informe del análisis de los riesgos en cuanto a las amenazas de la seguridad, vulnerabilidades e impactos potenciales y las medidas factibles de seguridad y control interno es preciso, completo y suficiente.

- Los problemas de seguridad y control interno se han tenido en cuenta apropiadamente en la documentación de diseño del sistema.

- La aprobación de la dirección de los controles existentes y planificados son suficientes y aportan beneficios apropiados comparados con los costos de compensación.

- Existen mecanismos disponibles para las pistas de auditoría o éstos pueden ser desarrollados para la solución identificada y seleccionada.

- Se ha tomado en cuenta un diseño amigable para el usuario para mejorar las habilidades finales de éste durante el diseño del sistema y el desarrollo del diseño de las pantallas, formato de informe, instalaciones de ayuda en línea, etc.

- Se han considerado aspectos ergonómicos durante el diseño y el desarrollo del sistema.

- Se han incluido aspectos de utilización de los usuarios (por ejemplo, tiempo de respuesta del sistema, capacidades de carga y descarga, e informes "ad hoc") en las especificaciones de requerimiento del sistema antes de su diseño y desarrollo.

- La identificación de todos los programas de software de los sistemas potenciales que satisfacen los requerimientos.

- La función de los servicios de información cumple con un conjunto común de procedimientos y estándares en la adquisición del hardware, software y los servicios relacionados con la tecnología de la información.

- El acuerdo de compra del software cuando sea requerido permite al usuario tener una copia del código fuente del programa, aplica las actualizaciones, renovaciones de la tecnología y los "fixes" son especificados en los documentos de adquisición.

- Los productos adquiridos son revisados y probados antes de ser usados y pagados completamente.

- El personal de programación trabaja sujetándose al mismo nivel de pruebas, revisión y aprobaciones que se exige a los programadores propios de la organización.

- La función para asegurar la calidad de la organización es responsable de la revisión y aprobación del trabajo llevado a cabo por los programadores.

- Es suficiente el plan de aceptación de las instalaciones, incluyendo los procedimientos y criterios.

- Es suficiente el plan específico de aceptación de la tecnología, incluyendo inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo.

Evaluación del riesgo
Llevando a cabo:

Una revisión detallada de:

- La identificación de soluciones automatizadas para satisfacer los requerimientos del usuario (incluyendo la definición de los requerimientos del usuario, formulación de los cursos de acción alternativos; identificación de los paquetes de software comercial y elaboración de los estudios de viabilidad del desarrollo tecnológico, de viabilidad económica, de la arquitectura de la información y de los análisis de los riesgos).

- La seguridad, los controles internos (incluyendo la consideración de diseños familiares al usuario, ergonomía, etc.) y las pistas de auditoría disponibles o "desarrollables" para la solución identificada y seleccionada.

- La selección e implementación del software del sistema.

- Las políticas y procedimientos existentes de desarrollo de software para la adecuación y el cumplimiento del control interno de la organización.

- La manera en que se administra el mantenimiento de terceros (mantenimientos de impresoras).

- La manera en que la programación de aplicación ha sido revisada y administrada.

- La identificación de todo lo especificado en el contrato por parte de la dirección de los servicios de información.

- El proceso de aceptación de la tecnología específica para asegurar que las inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo satisfacen los requerimientos especificados.

Identificando:

- Las deficiencias en la metodología del ciclo de vida de desarrollo de los sistemas de la organización.

- Soluciones que no satisfacen los requerimientos del usuario. • Tentativas de desarrollo de los sistemas que:

- No han considerado cursos alternativos, trayendo como resultado una solución más costosa.

- No han considerado los paquetes de software comercial que podrían haber sido implementados en menos tiempo y a un menor costo.

- No han considerado la viabilidad tecnológica de las alternativas o han considerado inapropiadamente la viabilidad tecnológica de la solución elegida, dando como resultado la incapacidad para implementar la solución como fue diseñada originalmente.

- Han hecho suposiciones equivocadas en el estudio de la viabilidad económica, dando como resultado la elección del curso de acción incorrecto.

- No han considerado el modelo de datos de la arquitectura de la información de la empresa, teniendo como resultado la elección del curso incorrecto.

- No han realizado análisis de los riesgos sólidos, y consecuentemente, no han identificado adecuadamente los riesgos (incluyendo amenazas, vulnerabilidades e impactos

potenciales) o los controles internos y de seguridad para reducir o eliminar los riesgos identificados.

- Están sobre controladas o controladas insuficientemente debido a que la economía de los controles y la seguridad son examinados inapropiadamente.
- No han contado con pistas de auditoría adecuadas.
- No han considerado los aspectos ergonómicos y de diseño familiar para el usuario, dando como resultado errores en la entrada de datos que podrían haber sido evitados.
- No han seguido el enfoque de adquisiciones establecido por la organización, dando como resultado costos adicionales creados por la organización.

CHAUDITORIA CONSULTORES S.A.		
Empresa a Auditar	**Objetivo de Control**	**Fecha Auditoria**
NATURA LACTEOS LTDA.	**DS5 GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS**	20 05 09
Auditores	Andrés Felipe Franco M. Mauricio Orozco Buitrago	Grupo 7
Responsables Auditados	Edwar Augusto Jaramillo Soto Maricela Zuloaga Sandra Milena Hernández Patiño	Grupo 2
El propósito de está auditoria es evaluar el objetivo de *Garantizar la seguridad de los sistemas* dentro de la empresa **Natura Lácteos.** Se desea verificar si la empresa **Natura Lácteos** administra identidades y autorizaciones a sus empleados y poseen documento de requerimientos, vulnerabilidades y amenazas de seguridad.		

Ejemplo auditoría 2

ORIGEN DE LA AUDITORIA.

La presente auditoria se realiza en cumplimiento de la solicitud que la empresa Natura Lácteos Ltda. Ha hecho a Chauditoria Consultores S.A, en su afán de detectar posibles síntomas de debilidad y de evaluar la eficiencia y efectividad en sus procesos de administración de datos.

1. GUÍA AUDITORA

Objetivos de Control

- Administrar las Medidas de Seguridad.
- Identificación, Autentificación y Acceso.
- Seguridad de Acceso a Datos en Línea.
- Dirección de Cuentas de Usuario.
- Revisión Gerencial de Cuentas del Usuario.
- Control del Usuario sobre Cuentas de Usuario.
- Vigilancia de Seguridad.
- Clasificación de Datos.
- Identificación Central y Gestión de los Permisos de Acceso.
- Informes sobre Actividades de Violación y Seguridad.
- Gestión de Incidentes.
- Autorización de Transacción.
- Protección de las Funciones de Seguridad.
- Gestión de Clave Criptográfica.
- Prevención, Detección y Corrección de Software Dañino.
- Arquitectura de Firewalls y Conexión con Redes Públicas.
- Protección del Valor Electrónico. 1.2. Obtención de Conocimiento

Recurso Humano a consultar:

Jefe área de seguridad informática Jefe de dirección de sistemas Administrador de la base de datos Jefe de departamento de desarrollo

Información a conocer

1. Políticas y procedimientos globales para la organización relacionados con la seguridad y el acceso a los sistemas de información.

2. Políticas y procedimientos de los servicios de información relacionados con seguridad y acceso a los sistemas de información.

3. Políticas y procedimientos relevantes, así como requerimiento de seguridad legales y regulatorios de los sistemas de información (por ejemplo, leyes, regulaciones, alineamientos, estándares industriales) incluyendo:

- Procedimientos de dirección de las cuentas del usuario.
- Política de seguridad del usuario o de protección de la información.
- Estándares relacionados con el comercio electrónico.
- Esquema de clasificación de los datos.
- Inventario del software de control de acceso.
- Plano de los edificios y habitaciones que contienen los recursos de los sistemas de información. • Inventario o esquema de los puntos de acceso físico a los recursos de los sistemas de información (por ejemplo, módems, líneas telefónicas y terminales remotas).
- Procedimientos de control de cambios del software de seguridad.
- Procedimientos de seguimiento, solución y priorización de problemas.
- Informes sobre violaciones a la seguridad y procedimientos de revisión administrativa.
- Inventario de los dispositivos de encriptación de datos y de los estándares de encriptación.
- Lista de los proveedores y clientes con acceso a los recursos del sistema.
- Lista de los proveedores de servicios utilizados en la transmisión de los datos.

- Prácticas de dirección de redes relacionadas con pruebas continúas de seguridad.
- Copias de los contratos de transmisión de datos de los proveedores de servicios.
- Copias de documentos firmados sobre seguridad y conocimiento de los usuarios.
- Contenido del material de formación sobre seguridad para nuevos empleados.
- Informes de auditoría de auditores externos, proveedores de servicios como terceros y dependencias gubernamentales relacionadas con la seguridad de los sistemas de información.

Aspectos a Evaluar
Evaluación de los controles, considerando si:

1. Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como los requerimientos de seguridad de los usuarios con propósitos de consistencia.
2. Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.
3. Se cuenta con un esquema de clasificación de los datos en operación que indica que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.
4. Se cuenta con perfiles de seguridad de usuario que representan “los menos accesos requeridos” y que muestran revisiones regulares de los perfiles por parte de la dirección.
5. La formación de los empleados incluye el conocimiento y concienciación sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.
6. Se cuenta con informes sobre violaciones de la seguridad y procedimientos formales de solución de problemas. Estos informes deberán incluir:

- Intentos no autorizados de acceso al sistema (sign on).
- Intentos no autorizados de acceso a los recursos del sistema.

- Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad.
- Privilegios de acceso a recursos por ID de usuario.
- Modificaciones autorizadas a las definiciones y reglas de seguridad.
- Accesos autorizados a los recursos (seleccionados por usuario o recurso).
- Cambio sobre el estado de la seguridad del sistema.
- Accesos a las tablas de parámetros de seguridad del sistema operativo. 7. Existen módulos criptográficos y procedimientos clave de mantenimiento, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión. 8. Existen estándares de dirección criptográfica claves tanto para la actividad centralizada como para la de los usuarios. 9. Los controles de cambios en el software de seguridad son formales y consistentes con los estándares normales de desarrollo y mantenimiento de los sistemas. 10. Los mecanismos de autenticidad en uso proveen las siguientes facilidades:
- Uso individual de los datos de autenticidad (ej., passwords y no reutilizables).
- Autentificación múltiple (ej., se utilizan dos o más mecanismos de autenticidad diferentes)
- Autenticidad basada en la política (ej., capacidad para especificar
- Procedimientos de autenticidad aparte en los eventos específicos).
- Autenticidad por demanda (ej., capacidad de volver a autentificar al usuario, en ocasiones, después de la autentificación inicial).

7. El número de sesiones concurrentes correspondientes al mismo usuario están limitadas.

8 Al entrar, aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión.

9. Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales.

10. Al lograrse la sesión con éxito, se despliega el historial de los intentos con éxito y fallidos de acceso a la cuenta del usuario.

11. La política de password incluye:

- Cambio inicial de la password la primera vez que se utiliza.
- Longitud adecuada mínima del password.
- La frecuencia obligatoria mínima de cambio de password.
- Verificación de la password en la lista de valores no permitidos (ej., verificación de diccionario).
- Protección adecuada para las passwords de emergencia.

12. El procedimiento formal para resolver los problemas incluye:

- ID de usuario suspendido después de 5 intentos de entrada fallidos.
- Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado de las entradas.
- El tiempo de autenticidad se limita a 5 minutos, después de los cuales se concluye la sesión.
- Se le informa al usuario la suspensión, pero no la razón de la misma.

13. Los procedimientos de entrada en el sistema incluyen el rechazo o autentificación base.

14. Los métodos de control de localización se utilizan para aplicar restricciones adicionales a las localizaciones específicas.

15. El acceso al servicio VoiceMail y el sistema PBX está controlado con los mismos controles físicos y lógicos de los sistemas.

16. Éxito un refuerzo de las políticas de posición delicada, incluyendo que:

- Se les pide a los empleados en puestos delicados que permanezcan fuera de la organización durante un periodo de tiempo cada año; que durante este tiempo su ID de usuario se suspenda; y las personas que los sustituyen en caso de advertir cualquier anormalidad de seguridad deben notificarla a la administración.
- La rotación de personal dentro de estas áreas delicadas se realiza de vez en cuando.

17. El hardware y software de seguridad así como los módulos de encriptación, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la “necesidad de conocimiento”.

18. El acceso a los datos de seguridad como a la gestión de la seguridad, datos de transacción delicados, passwords y claves de encriptación se limita a la base de la “necesidad de conocimiento”.

19. Se utilizan rutas de confianza para transmitir información delicada sin encriptar.

20. Para evitar la suspensión del servicio por ataques con faxes basura, se toman medidas de seguridad como:

- Evitar la publicación de números de fax fuera de la organización en la base de “necesidad de conocimiento”.
- Las líneas de fax utilizadas para solicitudes del negocio no se utilizan con otros fines.

21. Se han establecido con respecto a los virus de ordenadores las medidas de control preventivas y detectoras.

22. Para reforzar la integridad de los valores electrónicos, se toman las medidas siguientes:

- Se protegen las facilidades del lector de tarjeta contra la destrucción, publicación o modificación de la información de la misma.
- La información de la tarjeta (NIP y demás información) se protege contra la divulgación.
- Se evita la falsificación de las tarjetas.

23. Para reforzar la protección de la seguridad, se toman medidas como:

- El proceso de identificación y autentificación requiere ser repetido después de un cierto periodo de inactividad.
- Un sistema de candado, un botón de fuerza o una secuencia de salida que se puede activar cuando el terminal se deja encendido.

Evaluación de la suficiencia, probando que:

Los servicios de información cumplen con los estándares de seguridad relacionados con: ⎪ Autentificación y acceso. ⎪ Dirección de clasificación de los perfiles de usuario y seguridad de datos. ⎪ Informes y revisión gerencial de las violación e incidentes de seguridad. ⎪ Estándares criptográficos administrativos clave. ⎪ Detección de virus, solución y comunicación. ⎪ Clasificación y propiedad de los datos. ⎪ Existen procedimientos para la solicitud, establecimiento y mantenimiento del acceso de los usuarios al sistema. ⎪ Existen procedimientos para el acceso externo de los recursos del sistema, por ejemplo, "logon”, “ID”, “password” o contraseña y “dial back”. ⎪ Se lleva un inventario de los dispositivos del sistema para verificar su suficiencia. ⎪ Los

parámetros de seguridad del sistema operativo tienen como base estándares locales y del proveedor. ⎪ Las prácticas de dirección de la seguridad de la red son comunicadas, comprendidas e impuestas. ⎪ Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad. ⎪ Existen procedimientos de "logon" reales para sistemas, usuarios y para el acceso de proveedores externos. ⎪ Se emiten informes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes. ⎪ El acceso a las llaves y módulos criptográficos se limita a necesidades reales de consulta. ⎪ Existen llaves secretas para utilizar en transmisiones. ⎪ Los procedimientos para la protección contra el software dañino incluyen:

- Todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso.
- Existe una política por escrito para bajar archivos (downloads), aceptación o uso de aplicaciones gratuitas y compartidas y esta política está vigente.
- El software para aplicaciones altamente sensibles está protegido por MAC (Messsage Authentication Code - Código de Autentificación de Mensajes) o firma digital, y fallos de verificación para evitar el uso del software.
- Los usuarios tienen instrucciones para la detección e información sobre virus, como el desarrollo lento o crecimiento misterioso de archivos.
- Existe una política y un procedimiento vigente para la verificación de los disquetes externos al programa de compra normal de la organización.

Los firewalls poseen por lo menos las siguientes propiedades:

- Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles digitales, debe reforzarse físicamente).

Sólo se permitirá el paso del tráfico autorizado, como se define en la política de seguridad local.

- Los firewalls por si mismos son inmunes a la penetración.
- El tráfico se intercambia únicamente en firewalls a la capa de aplicación.
- La arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación.

- La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte.
- La arquitectura del firewall debe estar configurada de acuerdo a la "filosofía de arte mínima".
- La arquitectura del firewall debe desplegar una sólida autentificación para la dirección y sus componentes.
- La arquitectura del firewall oculta la estructura de la red interna.
- La arquitectura del firewall provee una auditoría de todas las comunicaciones hacia o a través del sistema del firewall y activará las alarmas cuando se detecte alguna actividad sospechosa.
- El host de la organización, que provee el soporte para las solicitudes de entrada al servicio de las redes públicas, permanece fuera del firewall.
- La arquitectura del firewall se defiende de los ataques directos (ej., a través del seguimiento activo de la tecnología de reconocimiento de los patrones y tráfico).
- Todo código ejecutable se explora en busca de códigos dañinos ej., virus, applets dañinos antes de introducirse en la red interna.

Evaluación del riesgo
Llevando a cabo:

1. Una revisión detallada de la seguridad de los sistemas de la información, incluyendo evaluaciones de penetración de la seguridad física y lógica de los recursos informáticos, de comunicación, etc.

2. Entrevistas a los nuevos empleados para asegurar el conocimiento y la concienciación en cuanto a seguridad y en cuanto a las responsabilidades individuales, por ejemplo, confirmar la existencia de declaraciones de seguridad firmadas y la formación para nuevos empleados en cuanto a seguridad.

3. Entrevistas a los usuarios para asegurar que el acceso está determinado tomando como base la necesidad ("menor necesidad") y que la precisión de dicho acceso es revisada regularmente por la gerencia.

Identificando:

- Accesos inapropiados por parte de los usuarios a los recursos del sistema.
- Inconsistencias con el esquema o inventario de redes en relación con puntos de acceso faltantes, accesorios perdidos, etc.
- Deficiencias en los contratos en cuanto a la propiedad y responsabilidades relacionadas con la integridad y seguridad de los datos en cualquier punto de la transmisión entre el envío y la recepción.
- Empleados no verificados como usuarios legítimos o antiguos empleados que cuentan aún con acceso.
- Solicitudes informales o no aprobadas de acceso a los recursos del sistema y Software de seguimiento de redes que no indican a la dirección de redes las violaciones de la seguridad.
- Defectos en los procedimientos de control de los cambios del software de redes.
- La no utilización de llaves secretas en los procedimientos de emisión y recepción de terceros.
- Deficiencias en los protocolos para generación de llaves, almacenamiento de distribución, entrada, uso, archivo y protección.
- La falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones.

CHAUDITORIA CONSULTORES S.A.				
Empresa a Auditar	**Objetivo de Control**	**Fecha Auditoria**		
NATURA LACTEOS LTDA.	**DS6 Identificar y Asignar Costos.**	20	05	09
Auditores	Andrés Felipe Franco M. Mauricio Orozco Buitrago	Grupo 7		
Responsables Auditados	Edwar Augusto Jaramillo Soto Maricela Zuloaga Sandra Milena Hernández Patiño	Grupo 2		

Ejemplo auditoría 3

ORIGEN DE LA AUDITORIA.

La presente auditoria se realiza en cumplimiento de la solicitud que la empresa Natura Lácteos Ltda. Ha hecho a Chauditoria Consultores S.A, en su afán de detectar posibles síntomas de debilidad y de evaluar la eficiencia y efectividad en sus procesos de administración de datos.

1. GUÍA AUDITORA

Objetivos de Control

- Elementos con Cargo.
- Procedimientos de Costo.
- Facturas de Usuarios y Procedimientos de Reembolso.

a. Obtención de Conocimiento
b. Recurso Humano a consultar: Gerencia General Jefe departamento de recursos humanos Jefe departamento de finanzas
c. Información a conocer:

1. Políticas y procedimientos generales para la organización relacionados con la planificación y la preparación del presupuesto.

2. Políticas y procedimientos de los servicios de información relacionados con la agregación de costos, facturación, metodología e informes de desarrollo y costos.

3. Los siguientes elementos de los servicios de información:

- Presupuesto actual y del año anterior.
- Informes de seguimiento de la utilización de los recursos de los sistemas de información.
- Datos fuente utilizados en la preparación de los informes de seguimiento.
- Metodología o algoritmo de asignación de costos.
- Informes históricos de facturación.

4. Los siguientes elementos de la dirección de usuarios:

- Presupuesto actual y del año anterior para los costos de los servicios de información.
- Plan de desarrollo y mantenimiento de los sistemas de información del año en curso.

- Gastos presupuestados para los recursos de los sistemas de información, incluyendo aquellos facturados o absorbidos.

Aspectos a Evaluar
Evaluación de los controles, considerando si:

Los servicios de información cuentan con un grupo responsable de la información y emisión de facturar a los usuarios.

Existen procedimientos que:

- Crean un plan anual de desarrollo y mantenimiento con la identificación de las prioridades por parte del usuario en cuanto al desarrollo, mantenimiento y gastos operacionales.

- Se permite una determinación de muy alto nivel en cuanto a en qué se gastan los recursos de los servicios de información.

- Generen un presupuesto anual para la función de los servicios de información, incluyendo: - Cumplimiento con los requerimientos de la organización en cuanto a la preparación de los presupuestos. - Consistencia en cuanto a qué costos deben ser asignados por los departamentos. - Comunicación de los costos históricos, previsión de los nuevos costos para la comprensión en cuanto a qué costos son incluidos y facturados. - Autorización de todos los costos presupuestados que deben ser asignados por la función de los servicios de información. - Frecuencia de la emisión de informes y cargo real de costos.

- Seguimiento de los costos asignados de todos los recursos de los sistemas de información pero sin limitarse a: - Hardware operacional. - Equipo periférico. - Utilización de telecomunicaciones. - Desarrollo y soporte de aplicaciones. - Generales administrativos. - Costos por servicios de proveedores externos. - Help desk. - Instalaciones y mantenimiento. - Costos directos e indirectos. - Gastos fijos y variables. - Costos discrecionales.

- Asisten en la emisión regular de informes en cuanto al rendimiento para las distintas categorías de costo.

- Informan a los usuarios en cuanto a mediciones (“benchmarks”) externas relacionadas con la efectividad de los costos, con el fin de permitir una comparación con respecto a las expectativas de la industria u otras fuentes alternativas de servicios.

- Permiten la modificación oportuna de la asignación de costos para reflejar los cambios en las necesidades de Natura Lácteos Ltda.
- Aprueban y aceptan formalmente los cargos al ser recibidos.
- Identifican las oportunidades de mejora de los servicios de información para reducir las facturaciones o para obtener un mejor valor por los cargos.
- Los informes aseguran que los elementos sujetos a costo son identificables, medibles y predecibles.
- Los informes capturan y resaltan los cambios en los componentes de costo.

Evaluación de la suficiencia, probando que:

Existe una metodología de asignación de costos, que los usuarios están de acuerdo en cuanto a su equidad, y que genera tanto costos como informes. Existe un programa de mejora para reducir costos o aumentar el resultado de los recursos de los sistemas de información. Los procesos de asignación e informe fomentan el uso más apropiado, efectivo y consistente de los recursos de las TI, éstos aseguran el tratamiento justo de los departamentos y sus necesidades, y los cargos reflejan los costos asociados con la prestación de servicios.

Evaluación del riesgo
Llevando a cabo:

- Un cálculo de la facturación a partir de datos fuente, a través de un algoritmo de asignación de facturación y dentro del flujo de informes.
- La precisión de los datos en el informe de resultados, como: - Utilización de la CPU. - Utilización de los periféricos. - Utilización de DASD. - Líneas de código escritas. - Líneas y páginas impresas. - Modificaciones de programas llevados a cabo. - Número de PCs, teléfonos, archivos de datos. - Consultas al help desk. - Número, duración de las transmisiones.
- La compilación de los datos fuente de recursos en el informe de resultado es correcta.
- Utilización de un algoritmo real para compilar y asignar costos a la facturación.
- La comprobación frecuente de la precisión de la facturación.

- Las facturaciones sean aprobadas.
- Se lleven a cabo revisiones consistentes de la facturación.
- El progreso en el plan de desarrollo de los usuarios tenga como base los costos expendidos.
- Se lleve a cabo una revisión de la distribución de informes en cuanto a la utilización e información sobre los costos.
- La satisfacción en cuanto a: - Lo razonable de la facturación comparada con las expectativas presupuestadas. - El plan de desarrollo anual con respecto a los costos. - Lo razonable de la facturación comparada con las fuentes alternativas, por ejemplo "benchmarks". - La comunicación de las tendencias que incrementaría o disminuiría la facturación. - Solución de las variaciones comparadas con la facturación esperada.

Identificando:

- Oportunidades para una mayor efectividad y propiedad de la metodología de facturación: - Incluyendo más componentes de costos. - Modificando los índices o unidades de medida de asignación de costos. - Modificando el algoritmo mismo de los costos. - Mecanizando o integrando la función de contabilidad y los informes generados por aplicaciones.
- Inconsistencias dentro del algoritmo de asignación.
- Inconsistencias de asignación.
- Oportunidades para la mejora de los recursos de los sistemas.
- Oportunidades para el usuario con el fin de aplicar de una mejor manera los recursos de los servicios de información para alcanzar los requerimientos de Natura Lacteos Ltda.
- Mejoras en la eficiencia de los procesos de recopilación, acumulación, asignación, informe y comunicación, los cuales se traducirán en un mejor resultado o menor costo para los usuarios de los servicios proporcionados.
- Que las tendencias de costos reflejadas por las variaciones y el análisis hayan sido traducidas a cargos modificados en los períodos siguientes y hayan sido reflejadas en la estructura de costos.

- Que existen oportunidades para hacer de los servicios de información un centro de provecho y beneficios al proporcionar servicios a otros usuarios internos o externos.

- Si la función de los servicios de información es un centro de provecho y beneficios, que la contribución de dichos beneficios se ajusten al plan y el presupuesto y que destaquen las oportunidades para aumentar los beneficios.

HERRAMIENTAS
ENCUESTA Y REVISION DOCUMENTAL:

- ¿La empresa cuenta con un plan para el manejo y los procedimientos relacionados con el seguimiento de la infraestructura tecnológica?

- ¿Cuáles son los cambios propuestos según costos y riesgos? ¿Quién da la debida aprobación?

- ¿Existe un cronograma a seguir para realizar las actualizaciones y revisiones a este?

- ¿Existen los objetivos a largo y corto plazo en el aspecto tecnológico en la organización?

- ¿Existe repositorio de información acerca del estado de las plataformas tecnológicas de la organización?

- ¿Cuál es la arquitectura de sistemas? ¿Cuál es la dirección tecnológica y cuáles son las estrategias de migración y contingencia?

- ¿Existen estándares tecnológicos para la organización, y son seguidos adecuadamente?

- ¿Los requerimientos de la organización son analizados y tenidos en cuenta para compras, y actualizaciones de hardware y software?

- ¿Existen roles bien definidos dentro del manejo y revisión de la infraestructura tecnológica?

- ¿Existen modelos de arquitectura de la información, modelo de diccionario de datos corporativo?

- ¿Existen documentos que den cuenta de los niveles de seguridad manejados para datos confidenciales?

- ¿Existen actas de reuniones para tratar el tema de la dirección tecnológica, cuáles son las tendencias futuras?

LISTA DE CHEQUEO

Aspecto a Considerar	Cumple	No Cumple	Observaciones
La empresa cuenta con suficientes y modernos recursos tecnológicos que apoyen el negocio.			
Se encuentran especificados los requerimientos en cuanto a tecnologías de información para la empresa.			
Existe un plan de infraestructura tecnológica que contemple costos, riesgos y requerimientos.			
Está conformado un consejo de arquitectura que dirija y monitoree las tendencias y regulaciones futuras.			
Se encuentran definidos claramente los estándares en cuanto a tecnologías de información para la empresa.			
Existen planes de contingencia ante los posibles riesgos para las tecnologías de información de la empresa.			

Lista de chequeo
REVISION DOCUMENTAL:

1. Políticas y procedimientos relacionados con el ciclo de vida de desarrollo de sistemas
2. Objetivos y planes a corto y largo plazo de tecnología de información.
3. Documentación seleccionada del proyecto incluyendo:
   - Definición de requerimientos.
   - Análisis de alternativas.
   - Estudios de factibilidad tecnológica
   - Estudios de factibilidad económica,
   - Análisis de modelos de datos de la empresa / arquitectura de información.

- Análisis de riesgos.
- Estudios de costo-efectividad sobre control/seguridad interna.
- Análisis de pistas de auditoría, estudios ergonómicos, y planes de aceptación y resultados de pruebas de instalaciones y tecnología específica.
- Pruebas de sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de rendimiento, pruebas de regresión, pruebas de aceptación del usuario, y finalmente, pruebas piloto del sistema total para evitar cualquier fallo inesperado del sistema.
- Documentación por escrito de requerimientos de usuario debidamente revisados y aprobados.
- Los servicios de programación se justifican a través de un requerimiento de servicios escrito por parte de un miembro designado de los servicios de información.
- Aprobación formal del estudio de los costos y beneficios por parte de la dirección.

1. Contratos seleccionados relacionados con la compra, desarrollo o mantenimiento de software en caso de ser requerido.

REVISIÓN DOCUMENTAL. (EXISTE O NO EXISTE)

- Procedimientos de dirección de las cuentas del usuario.
- Política de seguridad del usuario o de protección de la información.
- Estándares relacionados con el comercio electrónico.
- Esquema de clasificación de los datos.
- Inventario del software de control de acceso.
- Plano de los edificios y habitaciones que contienen los recursos de los sistemas de información.
- Inventario o esquema de los puntos de acceso físico a los recursos de los sistemas de información (por ejemplo, módems, líneas telefónicas y terminales remotas).

- Procedimientos de control de cambios del software de seguridad.
- Procedimientos de seguimiento, solución y priorización de problemas.
- Informes sobre violaciones a la seguridad y procedimientos de revisión administrativa.
- Inventario de los dispositivos de encriptación de datos y de los estándares de encriptación.
- Lista de los proveedores y clientes con acceso a los recursos del sistema.
- Lista de los proveedores de servicios utilizados en la transmisión de los datos.
- Prácticas de dirección de redes relacionadas con pruebas continúas de seguridad.
- Copias de los contratos de transmisión de datos de los proveedores de servicios.
- Copias de documentos firmados sobre seguridad y conocimiento de los usuarios.
- Contenido del material de formación sobre seguridad para nuevos empleados.
- Informes de auditoría de auditores externos, proveedores de servicios como terceros y dependencias gubernamentales relacionadas con la seguridad de los sistemas de información.

LISTADE
CHEQUEO

Aspecto a Considerar	Cumple	No Cumple	Observaciones
Se cuenta con plan de seguridad estratégico leyes, regulaciones, alineamientos, estándares industriales.			
Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.			
Se cuenta con un esquema de clasificación de los datos en operación que indica que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.			
Se cuenta con perfiles de seguridad de usuario que representan "los menos accesos requeridos" y que muestran revisiones regulares de los perfiles por parte de la dirección.			
La formación de los empleados incluye el conocimiento y concientización sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.			
Existen módulos criptográficos y procedimientos clave de mantenimiento, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión.			
Existen estándares de dirección criptográfica claves tanto para la actividad centralizada como para la de los usuarios.			
Se cuenta con un programa de concientización que fomente un ambiente de control positivo a través de toda la organización			
Se llevan a cabo revisiones regulares de las políticas Las políticas son claramente entendidas en todos los niveles de la organización			

Se hace un adecuado uso de las tecnologías de comunicación para la divulgación de políticas			
Se hace monitoreo de la duración de la implementación de políticas			
Las políticas son renovadas por lo menos una vez al año			
Las políticas se hacen cumplir a lo largo de toda la organización			
Se fomenta el buen uso de tales canales de comunicación			

Lista de chequeo 1

REVISIÓN DOCUMENTAL:

1. Hay políticas y procedimientos generales para la organización relacionados con la planificación y la preparación del presupuesto.

2. Hay políticas y procedimientos de los servicios de información relacionados con la agregación de costos, facturación, metodología e informes de desarrollo y costos.

3. A nivel de servicios de información: • Existe Informe Presupuesto actual y del año anterior.

- Existe Informes de seguimiento de la utilización de los recursos de los sistemas de información.
- Existe datos fuente utilizados en la preparación de los informes de seguimiento.
- Hay metodología o algoritmo de asignación de costos.
- Existen informes históricos de facturación.

4. A nivel de la dirección de servicios:

- Hay comprobantes de presupuesto actual y del año anterior para los costos de los servicios de información.
- Existe plan de desarrollo y mantenimiento de los sistemas de información del año en curso.
- Hay relaciones de gastos presupuestados para los recursos de los sistemas de información, incluyendo aquellos facturados o absorbidos.

LISTA DE CHEQUEO

Aspecto a Considerar	Cumple	No Cumple	Observaciones
Existen esfuerzos por parte de la gerencia de sistemas para Mejorar la relación costo/eficiencia de TI y su contribución a la rentabilidad del negocio			
Existe una relación claramente establecida entre la gerencia financiera y la gerencia de sistemas para mantener una contabilidad TI y un proceso de control de costos			
Existe un plan de aprendizaje formal para capacitar a los usuarios de los servicios TI y reducir el número de errores en costos ocasionados por estos.			
Existe un modelo de costos TI.			
Existe una política de mejoramiento continuo de los servicios de TI			
Existe una valoración completa de los riesgos en que incurre el negocio al hacer una nueva inversión en TI			

Lista de chequeo 2

RESULTADOS

ENCUESTA Y REVISION DOCUMENTAL:

- ¿La empresa cuenta con un plan para el manejo y los procedimientos relacionados con el seguimiento de la infraestructura tecnológica?
- No hay un plan que cumpla integralmente con este aspecto.
- ¿Cuáles son los cambios propuestos según costos y riesgos? ¿Quién da la debida aprobación?

- ¿Existe un cronograma a seguir para realizar las actualizaciones y revisiones a este?
- No existe tal cronograma
- ¿Existen los objetivos a largo y corto plazo en el aspecto tecnológico en la organización?
- Si existen dichos objetivos y están consignados en el PETI en la sección de Objetivos Estratégicos.
- ¿Existe repositorio de información acerca del estado de las plataformas tecnológicas de la organización?
- No existe este repositorio.
- ¿Cuál es la arquitectura de sistemas? ¿Cuál es la dirección tecnológica y cuáles son las estrategias de migración y contingencia?
- Se tiene definido el Hw y Sw con el que cuenta el área de sistemas pero no hay una estructura de redes y comunicaciones completa, por tal motivo no se cuenta con una arquitectura de sistemas clara. En cuanto al direccionamiento tecnológico, se puede decir que contamos con un Plan estratégico de TI el cual se toma como marco de referencia para apoyar las diferentes áreas de la organización, el plan mencionado tiene incluido un plan de contingencia pero aún no es lo suficientemente robusto, se incluyen medidas frente al “Corte de energía local o sectorial o global e incluso en caso de una variación del voltaje de la red pública o interna de energía, Borrado accidental o a propósito de archivos de datos o programas, Fallo de una CPU, Copias de Seguridad”. Por el momento se carece de un plan de migración.
- ¿Existen estándares tecnológicos para la organización, y son seguidos adecuadamente?
- No hay definidos estándares tecnológicos.
- ¿Los requerimientos de la organización son analizados y tenidos en cuenta para compras, y actualizaciones de hardware y software?

Este aspecto es tenido en cuenta en el plan estratégico de TI cuando se menciona las tendencias tecnologías pretendiendo aplicar las herramientas y tecnologías más apropiadas y que le sean útiles a la empresa.

- ¿Existen roles bien definidos dentro del manejo y revisión de la infraestructura tecnológica?

- La definición de roles está claramente establecido y soportado en la estructura organizacional del departamento de sistemas.

- ¿Existen modelos de arquitectura de la información, modelo de diccionario de datos corporativo?

- No hay definido ninguno de estos puntos.

- ¿Existen documentos que den cuenta de los niveles de seguridad manejados para datos confidenciales?

- No existen documentos que establezcan estos niveles de seguridad.

- ¿Existen actas de reuniones para tratar el tema de la dirección tecnológica, cuáles son las tendencias futuras?

Específicamente no se tienen actas sobre temas de dirección tecnológica.

Aspecto a Considerar	Cumple	No Cumple	Observaciones
La empresa cuenta con suficientes y modernos recursos tecnológicos que apoyen el negocio.	X		
Se encuentran especificados los requerimientos en cuanto a tecnologías de información para la empresa.		X	Solo sabemos con que recursos tecnológicos cuenta la empresa.
Existe un plan de infraestructura tecnológica que contemple costos, riesgos y requerimientos.		X	
Está conformado un consejo de arquitectura que dirija y monitoree las tendencias y regulaciones futuras.		X	Un consejo como tal no existe pero si se tiene conciencia y seguimiento a las tendencias en TI
Se encuentran definidos claramente los estándares en cuanto a tecnologías de información para la empresa.		X	
Existen planes de contingencia ante los posibles riesgos para las tecnologías de información de la empresa.	X		

Lista de chequeo 3

REVISIÓN DOCUMENTAL:

1. Políticas y procedimientos relacionados con el ciclo de vida de desarrollo de sistemas
Aunque el departamento hace sus propios desarrollos, no se tiene documentación sobre procedimientos y políticas relacionadas con el desarrollo de sistemas ni metodologías para el ciclo de vida del software.

2. Objetivos y planes a corto y largo plazo de tecnología de información.

Administrar efectivamente los procesos y recursos disponibles y futuros para alcanzar y mantener la excelencia en los servicios informáticos ofrecidos.

⎪ Estar preparados en por lo menos el 80% en el 2010 para la certificación de calidad ISO 9000 en los procesos y servicios informáticos ofrecidos por la Oficina Asesora de Informática y Telemática.

⎪ Apoyar la integración en el 2010 de al menos el 80% de las dependencias administrativas en lo relacionado con sus Sistemas de Información y herramientas de computación y telecomunicaciones.

⎪ Apoyar para que se garantice por lo menos en el 80% en el 2010 la operación y continuidad de los productos y servicios informáticos ofrecidos.

⎪ Implementar y mantener el esquema de seguridad informática requerido para generar confianza y transparencia en las operaciones informáticas para el 2009

⎪ Ejecutar al 2010 al menos el 70% de los proyectos de Tecnologías de Información y Telecomunicaciones – TIC definidos dentro del Plan de Desarrollo de la empresa.

⎪ Lograr y mantener un indicador de clima organizacional - ICO por lo menos del 70% al 2010, tratando de promover actitudes positivas del personal hacia su trabajo y la empresa.

⎪ Implementar al 2009 y mantener el esquema de seguridad informática requerido para generar confianza y transparencia en las operaciones informáticas

⎪ Lograr eficiencia en los procesos de prestación de servicios informáticos, de forma que se pueda generar ahorro y reducción de costos de hasta un 20% para finales del año 2009.

⎫ Establecer y mantener contacto permanente con las entidades proveedoras de Tecnologías de Información para la ejecución de los proyectos con el fin de mejorar el nivel de la organización para el año 2009.

⎫ Apoyar los procesos operativos, gerenciales y comerciales de la empresa, por lo menos un 50% para el 2009 para que se puedan seguir implementando los proyectos en el área de TIC's.

3. Documentación seleccionada del proyecto incluyendo:

- Definición de requerimientos. No hay documentación
- Análisis de alternativas. No hay documentación
- Estudios de factibilidad tecnológica. No hay documentación
- Estudios de factibilidad económica. No hay documentación
- Análisis de modelos de datos de la empresa / arquitectura de información. No hay documentación
- Análisis de riesgos. No hay documentación
- Estudios de costo-efectividad sobre control/seguridad interna. No hay documentación
- Análisis de pistas de auditoría, estudios ergonómicos, y planes de aceptación y resultados de pruebas de instalaciones y tecnología específica. No hay documentación
- Pruebas de sistema, pruebas de integración, pruebas de hardware y componentes, pruebas de procedimientos, pruebas de carga y estrés, pruebas de rendimiento, pruebas de regresión, pruebas de aceptación del usuario, y finalmente, pruebas piloto del sistema total para evitar cualquier fallo inesperado del sistema. No hay documentación
- Documentación por escrito de requerimientos de usuario debidamente revisados y aprobados. No hay documentación
- Los servicios de programación se justifican a través de un requerimiento de servicios escrito por parte de un miembro designado de los servicios de información. No hay documentación
- Aprobación formal del estudio de los costos y beneficios por parte de la dirección. No hay documentación

4. Contratos seleccionados relacionados con la compra, desarrollo o mantenimiento de software en caso de ser requerido.

Solo se tiene el objetivo:

"Garantizar por lo menos en el 80% en el 2010 la operación y continuidad de los productos y servicios informáticos ofrecidos." Y es en este donde se tiene como proyecto "Definir políticas e implementar normas y procedimientos para la consolidación de las compras de elementos de Tecnologías de Información y Comunicaciones – TIC, el manejo de proyectos corporativos y la definición y utilización de estándares tecnológicos."

REVISIÓN DOCUMENTAL. (EXISTE O NO EXISTE)

- Procedimientos de dirección de las cuentas del usuario. No existe
- Política de seguridad del usuario o de protección de la información. Existe
- Estándares relacionados con el comercio electrónico. No Existe
- Esquema de clasificación de los datos. No Existe
- Inventario del software de control de acceso. Existe
- Plano de los edificios y habitaciones que contienen los recursos de los sistemas de información. No Existe
- Inventario o esquema de los puntos de acceso físico a los recursos de los sistemas de información (por ejemplo, módems, líneas telefónicas y terminales remotas). No Existe
- Procedimientos de control de cambios del software de seguridad. No Existe
- Procedimientos de seguimiento, solución y priorización de problemas. No Existe
- Informes sobre violaciones a la seguridad y procedimientos de revisión administrativa. No Existe
- Inventario de los dispositivos de encriptación de datos y de los estándares de encriptación. No Existe
- Lista de los proveedores y clientes con acceso a los recursos del sistema. No Existe

- Lista de los proveedores de servicios utilizados en la transmisión de los datos. No Existe
- Prácticas de dirección de redes relacionadas con pruebas continúas de seguridad. No Existe
- Copias de los contratos de transmisión de datos de los proveedores de servicios. No Existe
- Copias de documentos firmados sobre seguridad y conocimiento de los usuarios. No Existe
- Contenido del material de formación sobre seguridad para nuevos empleados. No Existe
- Informes de auditoría de auditores externos, proveedores de servicios como terceros y dependencias gubernamentales relacionadas con la seguridad de los sistemas de información. No Existe

LISTA DE CHEQUEO

Aspecto a Considerar	Cumple	No Cumple	Observaciones
Se cuenta con plan de seguridad estratégico leyes, regulaciones, alineamientos, estándares industriales.		X	
Se cuenta con una organización de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.		X	
Se cuenta con un esquema de clasificación de los datos en operación que indica que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.		X	
Se cuenta con perfiles de seguridad de usuario que representan "los menos accesos requeridos" y que muestran revisiones regulares de los perfiles por parte de la dirección.	X		Pero no regulaciones de los perfiles de la dirección.
La formación de los empleados incluye el conocimiento y concientización sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus.	X		
Existen módulos criptográficos y procedimientos clave de mantenimiento, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión.		X	
Existen estándares de dirección criptográfica claves tanto para la actividad centralizada como para la de los usuarios.		X	
Se cuenta con un programa de concientización que fomente un ambiente de control positivo a través de toda la organización		X	No hay un programa como tal pero dentro de la formación que se le da a los empleados se fomentan actitudes positivas hacia la organización y sus

			compañeros que generan ambientes de trabajo agradables para todos
Se llevan a cabo revisiones regulares de las políticas Las políticas son claramente entendidas en todos los niveles de la organización Se hace un adecuado uso de las tecnologías de comunicación para la divulgación de políticas	X		
Se hace monitoreo de la duración de la implementación de políticas		X	
Las políticas son renovadas por lo menos una vez al año	X		
Las políticas se hacen cumplir a lo largo de toda la organización	X		
Se fomenta el buen uso de tales canales de comunicación	X		

Lista de chequeo 4
REVISICIÓN DOCUMENTAL:

1. Hay políticas y procedimientos generales para la organización relacionados con la planificación y la preparación del presupuesto. R: Existen – soporte (área financiera).

2. Hay políticas y procedimientos de los servicios de información relacionados con la agregación de costos, facturación, metodología e informes de desarrollo y costos. R: No hay conocimiento de ellas.

3. A nivel de servicios de información:

- Existe Informe Presupuesto actual y del año anterior. R: No.
- Existe Informes de seguimiento de la utilización de los recursos de los sistemas de información. R: No.
- Existe datos fuente utilizados en la preparación de los informes de seguimiento. R: No.
- Hay metodología o algoritmo de asignación de costos. R: No.
- Existen informes históricos de facturación. R: No.

4. A nivel de la dirección de servicios:

- Hay comprobantes de presupuesto actual y del año anterior para los costos de los servicios de información. R: No.
- Existe plan de desarrollo y mantenimiento de los sistemas de información del año en curso. R: Existe el plan de desarrollo, el plan de mantenimiento no existe, sin embargo está incluido en los objetivos estratégicos.
- Hay relaciones de gastos presupuestados para los recursos de los sistemas de información, incluyendo aquellos facturados o absorbidos. R: No.

LISTA DE CHEQUEO

Aspecto a Considerar	Cumple	No Cumple	Observaciones
Existen esfuerzos por parte de la gerencia de sistemas para Mejorar la relación costo/eficiencia de TI y su contribución a la rentabilidad del negocio	**Si**		**Definido en los proyectos de TI**
Existe una relación claramente establecida entre la gerencia financiera y la gerencia de sistemas para mantener una contabilidad TI y un proceso de control de costos	**No**		
Existe un plan de aprendizaje formal para capacitar a los usuarios de los servicios TI y reducir el número de errores en costos ocasionados por estos.	**Si**		**Definidos en el PETI**
Existe un modelo de costos TI.	**No**		
Existe una política de mejoramiento continuo de los servicios de TI			**Visión**
Existe una valoración completa de los riesgos en que incurre el negocio al hacer una nueva inversión en TI	**No**		

Lista de chequeo 5

INFORME

CHAUDITORIA CONSULTORES S.A.				
Empresa a Auditada	INFORME AUDITORIA PROCESOS PO3, AI1, DS5, DS6	Fecha Informe		
NATURA LACTEOS LTDA.		27	05	09
Auditores	Andrés Felipe Franco M. Mauricio Orozco Buitrago	Grupo 7		
Responsables Auditados	Edwar Augusto Jaramillo Soto Maricela Zuloaga Sandra Milena Hernández Patiño	Grupo 2		

Informe 1

Determinar la Dirección Tecnológica
Objetivo

Determinar la dirección tecnológica de la empresa Natura Lácteos para así permitir dar soporte tecnológico adecuado para una empresa de esta índole. Se busca los sistemas del negocio, la arquitectura de la información y los estándares tecnológicos con que cuenta Natura Lácteos. Para detectar el incumplimiento de los estándares tecnológicos, desviaciones con respecto al plan de infraestructura tecnológica.

Hallazgos

No existe un proceso para la creación y la actualización regular del plan de infraestructura tecnológica para confirmar que los cambios propuestos están siendo examinados antes de evaluar los costos y riesgos inherentes.

No hay un cronograma que estime la actualización y revisión de la infraestructura tecnológica de la organización.

No existe un repositorio de información acerca del estado de las plataformas tecnológicas de la organización.

No hay estrategias bien definidas para la migración y contingencia que deben ser contemplados en el plan estratégico de infraestructura tecnológica. La dirección de los servicios de información comprende el proceso de evaluar sistemáticamente, por ejemplo, redundancia, resistencia, adecuación y capacidad evolutiva de la infraestructura.
No hay modelo de la arquitectura de la información ni modelo de diccionario de datos corporativo, en los sistemas de información asociados y en los planes a largo y corto plazo de la tecnología de la información. No existe documentación que dé cuenta de los niveles de seguridad y confidencialidad de los datos.

Se encuentran definidos objetivos estratégicos de TI que buscan por medio de la adquisición de nuevas tecnologías satisfacer las metas empresariales.

Conclusión

No se logra identificar en el plan de TI qué tecnologías tienen el potencial de crear oportunidades de negocio dado que este no abarca la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.

Cabe resaltar el hecho de que se han definido algunos objetivos estratégicos de TI alineados con las metas empresariales que deben estar apoyados en un plan de dirección tecnológica el cual no se encuentra bien definido.

Recomendaciones
Realizar investigación sobre las tecnologías apropiadas para la empresa y adecuarlas bajo el modelo de dirección tecnológica implantado hasta ahora, guiándose en los siguientes procesos:

- Elaborar y mantener plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. Este se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones.

- Establecer un foro o un consejo tecnológico que brinden directrices tecnológicas, asesoría sobre los productos de la infraestructura y guías sobre la selección de la tecnología, y medir el cumplimiento de estos estándares y directrices.

AI1 Identificar Soluciones Automatizadas
Objetivo

Definir y dar mantenimiento de los requerimientos técnicos y funcionales de Natura Lácteos e Identificar los riesgos asociados con los procesos de negocio determinando los cursos de acción alternativos.

Hallazgos

No se encuentra definida una metodología de desarrollo de software ni políticas y procedimientos relacionados con el ciclo de vida de desarrollo de los sistemas desarrollados por la empresa; por lo que no se lleva un adecuado seguimiento de los requerimientos de negocio tanto funcionales como técnicos (definición, actualización, cumplimiento).

Los objetivos y planes a corto y largo plazo de la tecnología de la información se tienen considerados de acuerdo a un plan de metas el cual provee un diagnóstico y alcance de lo que se necesita en la organización.

No existen estudios de factibilidad de proyectos tecnológicos así como estudios de factibilidad económica y de alternativas.

No se han realizado análisis de los riesgos sólidos, y consecuentemente, no han identificado adecuadamente los riesgos (incluyendo amenazas, vulnerabilidades e impactos potenciales) o los controles internos y de seguridad para reducir o eliminar los riesgos identificados dentro de las soluciones automatizadas.

Conclusión

No se logra identificar dentro de la empresa Natura Lácteos la definición de requerimientos técnicos y funcionales del negocio dado que no existe una metodología a seguir ni una propia; por la misma razón no existe análisis de riesgos asociados con los procesos del negocio ni políticas o estándares de evaluación de factibilidad de proyectos tecnológicos, costos y alternativas.

Recomendaciones

Los costos de las soluciones automatizadas deben ser planeados, por tanto se debe diseñar un plan de costos para estas, además debe existir documentación formal de aprobación por parte de la dirección que contemple los costos y beneficios de las aplicaciones automatizadas.

Desarrollar un estudio de factibilidad que examine la posibilidad de implantar los requerimientos. Debe identificar los cursos alternativos de acción para el software, hardware, servicios y habilidades que satisfagan los requerimientos establecidos, tanto funcionales como técnicos, y evaluar la factibilidad tecnológica y económica (costo potencial y análisis de beneficios) de cada uno de los cursos de acción identificados en el contexto de inversión en TI

Diseñar un plan de gestión de requerimientos de servicios debidamente documentados y con sus respectivos responsables. Debe realizarse un plan de contratación de soluciones automatizada que dé cuenta en caso de requerirse la compra de productos de software que hay cumplimiento con las políticas de adquisición de la organización definiendo el marco de referencia para la solicitud de propuesta, la selección del proveedor de software y la negociación del contrato; por lo que puede presentarse que las instancias en las que se ha aceptado una tecnología específica, pero que no se han llevado a cabo adecuadamente inspecciones, pruebas de funcionalidad y pruebas de carga de trabajo, teniendo como resultado que la tecnología no satisface los requerimientos del usuario y no cumple con los términos del contrato.

DS5 Garantizar la Seguridad de los Sistemas
Objetivo

Garantizar la seguridad de los sistemas dentro de la empresa Natura Lácteos. Se desea verificar si la empresa Natura Lácteos administra identidades y autorizaciones a sus empleados y poseen documento de requerimientos, vulnerabilidades y amenazas de seguridad.

Hallazgos

Aunque se pretende la concientización en los empleados y funcionarios de la empresa sobre las políticas, estándares y convenciones en seguridad informática hacen falta estudios y la definición de políticas referentes a la seguridad en TI.

No se cuenta con plan de seguridad estratégico, leyes, regulaciones, alineamientos, estándares industriales; no existen políticas de control de accesos, a equipos administrativos, a diferentes páginas web, no hay políticas de la adquisición de software ni de sus actualizaciones.

No se cuenta con un esquema de clasificación de los datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido. No se emiten informes sobre violaciones de seguridad en cuanto a la oportunidad, precisión y respuesta a incidentes.

No hay estándares de encriptación; el hardware y software no están protegidos contra la intromisión o divulgación de información. El acceso a los datos de seguridad como a la gestión de la seguridad, datos de transacción delicados, passwords y claves de encriptación son limitados.

Conclusión

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Aunque Natura Lácteos Ltda. Establece roles y responsabilidades de seguridad dentro de la empresa no define ni mantiene un plan estratégico de seguridad en TI. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad

Recomendaciones

Administrar la seguridad de TI al nivel más apropiado dentro de la organización, de manera que las acciones de administración de la seguridad estén en línea con los requerimientos del negocio, guiándose en los siguientes procesos:

- Elaborar un plan de seguridad estratégico, leyes, regulaciones, alineamientos y estándares industriales. Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.

- Realizar monitoreos de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados.

- Todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, operación del sistema, desarrollo y mantenimiento) deben ser identificables de manera única. Los derechos de acceso del usuario a sistemas y datos deben estar alineados con necesidades de negocio definidas y documentadas y con requerimientos de trabajo.

- Garantizar que la tecnología importante relacionada con la seguridad no sea susceptible de sabotaje y que la documentación de seguridad no se divulgue de forma innecesaria, es decir, que mantenga un perfil bajo.

- Realizar la planificación de estándares de los módulos de dirección criptográfica, claves tanto para la actividad centralizada como para el usuario, para reforzamiento de la protección y seguridad.

- Realizar un estudio detallado de los estándares de comercio electrónico que se utilicen dentro de Natura Lácteos Ltda. Con los debidos accesos apropiados por parte de los usuarios a los recursos del sistema.

DS6 Identificar y Asignar Costos
Objetivo

Determinar el nivel de seguimiento sobre la asignación de costos en TI basado en políticas y estrategias que permitan la vinculación de los servicios de TI a los procesos de negocio.

Hallazgos

No existe un modelo de costos de TI que incluya costos directos, indirectos y fijos de los servicios de TI. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa, lo que claramente no se detecta en Natura Lácteos Ltda.

No se genera un presupuesto anual para la función de los servicios de información, que incluya aspectos como: cumplimiento con los requerimientos de la organización en cuanto a la preparación de los presupuestos; consistencia en cuanto a qué costos deben ser asignados por los departamentos; comunicación de los costos históricos, previsión de los nuevos costos para la comprensión en cuanto a qué costos son incluidos y facturados; autorización de todos los costos presupuestados que deben ser asignados por la función de los servicios de TI.

No hay comprobantes de presupuesto actual y del año anterior para los costos de los recursos de los sistemas y servicios de TI.

Conclusión

Se hace obvia la necesidad de un sistema justo y equitativo para asignar costos de TI en la empresa Natura Lácteos Ltda., este requiere de una medición precisa y un acuerdo con los usuarios del negocio sobre una asignación justa.

Recomendaciones

Si la función de los servicios de información es un centro de provecho y beneficios, la contribución de dichos beneficios deben estar ajustados al plan y el presupuesto empresarial y que destaquen las oportunidades para aumentar los beneficios y así poder capacitar a los usuarios de los servicios de TI con tal sentido de pertenencia que ayude a reducir y corregir a tiempo errores en costos ocasionados por dichos usuarios. Dado esto se recomienda:

- Elaborar un modelo de costos de TI que garantice que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos; además debe estar alineado con los procedimientos de contabilización de costos de la empresa.

- Registrar y asignar los costos actuales de acuerdo con el modelo de costos definido. Las variaciones entre los presupuestos y los costos actuales deben analizarse y reportarse de acuerdo con los sistemas de medición financiera de la empresa.

- Revisar y comparar de forma regular lo apropiado del modelo de costos/recargos para mantener su relevancia para el negocio en evolución y para las actividades de TI.

Nivel de Madurez de la Empresa

La empresa Natura Lácteos entra a clasificarse como un nivel 1 Inicial/Ad Hoc en los procesos PO3, AI1, DS5 y DS6, analizados en esta auditoría. Pues si bien se reconoce la necesidad de estructurar las funciones de dirección de TI, identificar soluciones automatizadas para la satisfacción de requerimientos del negocio, definir y garantizar las políticas de seguridad de los sistemas y se reconoce también la necesidad de especificar estándares y políticas de control sobre la asignación de todos los costos de TI, las operaciones son de naturaleza reactiva, se toman acciones de manera informal y el procesamiento de peticiones se acepta sin validación previa, no se mide la seguridad de TI, no hay una distribución de costos por usuario, cliente, departamento, grupos de usuarios, funciones de servicio, proyectos o entregables y la dirección tecnológica está impulsada por los planes evolutivos, con frecuencia contradictorios, del hardware, del software de sistemas y de los proveedores de software aplicativo.

5. PISTAS DE APRENDIZAJE

Tenga en cuenta que: la función de un auditor no es la de buscar los errores o no conformidades de la Organización auditada, sino de ayudarles a encontrar sus debilidades y que creen planes de mejora.

No se puede olvidar: que cuando la auditoría requiere de mayores conocimientos a los que tiene el auditor en curso, es totalmente válido hacer uso de un experto en el tema para que la evaluación sea más verídica y fiable posible.

Tenga en cuenta: que cuando en una auditoría no se encuentra algún procedimiento realizado de la manera que se espera, pero se cuenta con el plan de mejora para éste, no se debe reportar como una no conformidad puesto que la organización ya es consciente de dicha falencia, pero además ya tiene un plan de contingencia para la misma.

Tener en cuenta: que las investigaciones previas a la auditoría, aportan información y material fundamental para el proceso de la auditoría en sí.

No olvidar que: un auditor no debe realizar informes basándose en supuestos o rumores, pues los resultados no serán fieles a la realidad de la organización. Siempre debe haber un soporte formal de la compañía para cualquier informe, o en su defecto no haberlo para así levantar los planes de contingencia.

Tener muy presente que: los auditados no siempre responden claramente a las preguntas realizadas por el auditor, y esto se puede deber a que la persona no comprende los conceptos de la manera que le fueron preguntados, luego es muy bueno repetir sigilosamente la pregunta de una manera más sencilla, para verificar nuevamente la existencia o no de los requerido.

Traer siempre a la memoria: el propósito de la auditoría. Este es la carta de navegación del proceso a auditar.

Tener en cuenta que: la selección del personal auditado debe hacerse con la certeza que son las personas que pueden dar claramente respuesta a los procesos de la organización. Siempre se encontrarán personas en el área a auditar que no son las más idóneas para ser auditadas aunque allí laboren.

6. GLOSARIO

AUDITADO: persona de la organización que es seleccionada por el auditor para participar en el proceso de evaluación de algún proceso de la organización.

AUDITOR: persona idóneamente formada en el campo seleccionado para realizar la evaluación y coherencia de los procesos de la organización.

AUDITORÍA: proceso de evaluación de las actividades y procesos de una organización.

CONFORMIDAD: hallazgo de cumplimiento con los criterios de evaluación solicitados por el auditor.

CONTROLES: actividades de aseguramiento y verificación de que lo planeado si se realice conforme a lo planeado en la organización.

INFORME DE AUDITORÍA: Reporte escrito de los hallazgos encontrados durante el proceso de auditoría.

LISTA DE CHEQUEO: listados de preguntas que se hacen durante la auditoría para ir verificando el cumplimiento o no de las actividades del proceso.

NO CONFORMIDAD: Hallazgo de incumplimiento a los criterios de evaluación solicitados por el auditor.
OBSERVACIÓN: es una anotación a un hallazgo encontrado por el auditor, pero que su no cumplimiento no afecta el proceso auditado como tal.

SEGUIMIENTO: actividades de verificación relacionadas con el informe de auditoría.

SISTEMA: Conjunto de elementos interrelacionados entre sí para llegar a un fin común o propósito.

7. BIBLIOGRAFÍA

Tamayo, A. (2001).Auditoría de Sistemas: Una visión Práctica. [En línea]. Consultado: [23, octubre, 2011] Disponible en: http://books.google.es/books?id=HdtpS3UBCuMC&printsec=frontcover&dq=auditoria+de+sistemas&hl=es&ei=fJyDTsmHLYy4tgeA8pTtAQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CDQQ6AEwAA#v=onepage&q&f=false

Champlain, J. (2003). Auditing Information Systems. (Second Edition). [En línea]. Consultado: [27, Octubre, 2011] Disponible en: http://books.google.es/books?id=LJmzMzkUuHoC&printsec=frontcover&dq=systems+audit&hl=es&ei=yImjTuXTHcmXtwen7PmoBQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CDgQ6AEwAA#v=onepage&q=systems%20audit&f=false

Dube, D P. Y Gulati, VP. (2005). Information System Audit and Assurance.[En Línea]. Consultado: [27, octubre, 2011]. Disponible en: http://books.google.es/books?id=1cIQS6aCPQwC&printsec=frontcover&dq=systems+audit&hl=es&ei=yImjTuXTHcmXtwen7PmoBQ&sa=X&oi=book_result&ct=result&resnum=2&ved=0CD0Q6AEwAQ#v=onepage&q=systems%20audit&f=false

Valverde, O. Manual de Auditoría de Sistemas. En: http://www.slideshare.net/oskr12381/mdulo-auditoria-de-sistemas

Trabajo de Campo: Auditoría Realizada por el grupo 7 al grupo 2. Desde: http://ingenieria.ucaldas.edu.co/auditoria/index.php/Grupo_7

Auditoría de Sistemas. De: 123 Innovation Group, S.L. Auditores y consultores en seguridad, disponibilidad, continuidad, integridad y confidencialidad informática. [En línea]. Desde: http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/

TABLA REFERENCIA GRÁFICOS E IMÁGENES

Nombre imagen	Dirección	Autor
Video Intro Unidad 1	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Definición Auditoría de Sistemas	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Objetivos Generales de la Auditoría	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Función Auditoría en la Organización	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Video Intro Unidad2	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Pasos previos a una auditoría (mapa)	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Investigación Preliminar	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Recomendaciones para el auditor	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Tipos de Controles	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Objetivos Planeación de la Auditoría	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Fuentes para la Información	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Prueba Inicial Unidad 3	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Video Intro Unidad3	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Fases para la Auditoría de Sistemas	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Preguntas para el seguimiento	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Normas para el seguimiento	Módulo Auditoría de Sistemas	Elizabeth Díaz Duque
Ejemplo de Auditoria	http://ingenieria.ucaldas.edu.co/auditoria/index.php/Grupo_7	Universidad de Caldas
Ejemplo Auditoría 1	http://ingenieria.ucaldas.edu.co/auditoria/index.php/Grupo_7	Universidad de Caldas
Ejemplo Auditoría 2	http://ingenieria.ucaldas.edu.co/auditoria/index.php/Grupo_7	Universidad de Caldas
Lista de Chequeo	http://ingenieria.ucaldas.edu.co/auditoria/index.php/Grupo_7	Universidad de Caldas
Lista de Chequeo1	http://ingenieria.ucaldas.edu.co/	Universidad de Caldas

	auditoria/index.php/Grupo_7	
Lista de Chequeo2	http://ingenieria.ucaldas.edu.co/ auditoria/index.php/Grupo_7	Universidad de Caldas
Lista de Chequeo3	http://ingenieria.ucaldas.edu.co/ auditoria/index.php/Grupo_7	Universidad de Caldas
Lista de Chequeo4	http://ingenieria.ucaldas.edu.co/ auditoria/index.php/Grupo_7	Universidad de Caldas
Lista de Chequeo5	http://ingenieria.ucaldas.edu.co/ auditoria/index.php/Grupo_7	Universidad de Caldas
Informe 1	http://ingenieria.ucaldas.edu.co/ auditoria/index.php/Grupo_7	Universidad de Caldas