UNIVERSIDAD TECNOLÓGICA DE PANAMÁ

FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

DEPARTAMENTO DE ARQUITECTURA Y REDES DE COMPUTADORAS

LICENCIATURA EN REDES INFORMÁTICAS

ASIGNATURA:

AUDITORÍA DE REDES

DR. VLADIMIR VILLARREAL

2016

CONTENIDO

I. IMPORTANCIA DE LA AUDITORÍA

OBJETIVOS:

- Reconocer e identificar los diferentes conceptos de auditoría, así como los elementos que la formaron, para comprender su importancia y vigencia actual.
- Explicar los fundamentos básicos de la Auditoría

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Explicar el concepto general de Auditoría y su importancia, el proceso de Control que es establecido por la administración con la finalidad de lograr los objetivos de la entidad. Además de detallar los tipos de auditoria informática y sus características principales.

I. Importancia de la Auditoría

1.1 El proceso Administrativo y la Auditoría

El auditor deberá evaluar los métodos de control utilizados por la administración para supervisión y seguimiento en relación con el cumplimiento de los objetivos del negocio, incluyendo la función de auditoria interna. Entre los puntos que el auditor deberá revisar están:

a) Existencia de un proceso formal de planeación y presupuesto como una herramienta para vigilar los resultados y objetivos del negocio.

b) Verificar la existencia de un departamento de auditoria interna. En caso de que este exista, se deberá de considerar si este realiza actividades que puedan atenuar situaciones de riesgo en el ambiente de control.

c) El auditor deberá vigilar que se cumplan las políticas y prácticas de personal, por lo que deberá de contar con procedimientos y políticas por escrito para reclutar, contratar, capacitar, evaluar, promover, compensar y proporcionar al personal los recursos necesarios de manera que pueda cumplir con sus responsabilidades que le sean asignadas, a su vez deberá de desarrollar descripciones de trabajo las cuales deberán de ser adecuadas para cada puesto, deberá contar con canales adecuados de comunicación hacia todos los niveles de personal, que proporcionen un flujo oportuno y eficiente de información de carácter general, de negocios, técnica, etcétera. Se deberá de mantener un programa periódico, de revisiones de los conceptos señalados.

d) Es de suma importancia que la entidad cuente con los canales de comunicación adecuados con sus clientes, proveedores, acreedores financieros los cuales le permitan recibir información relativa a las transacciones realizadas con ellos, para lograr lo anterior deberán de tener establecidos procedimientos para asegurar que personal independiente al área afectada dé el seguimiento a las comunicaciones que son recibidas, para que en su caso se efectúen las correcciones que sean necesaria.

1.2 Conceptos de Control

Un procedimiento de control es aquel que es establecido por la administración con la finalidad de lograr los objetivos de la entidad, porque, aunque existen políticas o procedimientos de control, no significa que estén operando correctamente. En este caso la intervención del auditor será la de corroborar que estén dando dichos procedimientos los resultados esperados. El auditor para evaluar la estructura del control interno deberá de asegurarse que los procedimientos de control se cumplan, dicha valoración se deberá de llevar a cabo al momento de la toma de decisiones. Pueden ser supervisiones independientes o una combinación de ambas. Para una mejor comprensión al momento de la toma de decisiones, los funcionarios deberán revisar que el control interno establecido se haya completado. El auditor deberá garantizar que funcionarios independientes participen en la vigilancia de las operaciones, la evaluación que realicen deberá ser efectuada conforme a los procedimientos establecidos. Es importante que al momento de efectuar este mecanismo de vigilancia se documente especificando quienes y en qué momento la realizan, ya que esto le permitirá al auditor determinar la oportunidad de aplicación de los procedimientos. El auditor deberá de considerar el grado de complejidad de la situación que está analizando, por lo que en este rubro podrá analizar dicha situación mediante la elaboración de cuestionarios a los funcionarios con el propósito de obtener una evaluación relacionada con la efectividad tanto de los mecanismos de control como de los procedimientos realizados. El auditor en esta evaluación deberá de formarse un juicio profesional en relación a la posibilidad de que existan situaciones no previstas o un mal manejo de la administración, es por ello que el auditor en sus papeles de trabajo deberá observar un adecuado entendimiento en donde cuestione condiciones tales como la naturaleza, oportunidad y alcance de las pruebas de la auditoria que se aplicará. Esta evaluación constituye la estructura del control interno por lo que forma parte clave del trabajo de auditoría, en la cual su juicio tendrá un papel relevante, ya que s entendimiento del ambiente de control, del sistema de comunicación y de los procedimientos de control serán fundamentales para el logro total o parcial de los objetivos que se plantearon. Así mismo el auditor deberá considerar aquellas circunstancias que afectarán la operación de la misma para procesarlas adecuadamente, entre estos riesgos se incluyen nuevas disposiciones legales, reformas, nuevas

tecnologías, sistemas de información, reestructuras corporativas, cambios de administración, nuevas actividades entre otras. Una vez que haya sido aprobada la evaluación de control interno, el auditor diseñará la evaluación de las pruebas o de los procedimientos verificando la aplicación de estos en el ámbito de la organización. Las pruebas de cumplimiento son el medio de comprobación de que los procedimientos de control interno estuvieron operando con efectividad durante el periodo auditado.

1.2.1 Controles Internos

El control interno es la implementación de medidas que se establecen en las empresas, con el fin de contar con instrumentos tendientes a salvaguardar la integridad de los bienes institucionales y así ayudar a la administración y cumplimiento correctos de las actividades y operaciones de las empresas. Con la implantación de tales medidas se pueden conseguir los siguientes beneficios:

• Proteger y salvaguardar los bienes de la empresa y a su personal.

• Prevenir y, en su caso, descubrir la presencia de fraudes, robos y acciones dolosas.

• Obtener la información contable, financiera y administrativa de manera confiable y oportuna.

• Promover el desarrollo correcto de las funciones, operaciones y actividades de la empresa.

Definiciones de control interno

Para entender cómo funciona el control interno en las empresas, se presentan las aportaciones de algunos autores al respecto:

JOSÉ ANTONIO ECHENIQUE

“El control interno comprende el plan de organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus actividades, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración.”

HOLMES R. ARTHUR

“El control interno es una función de la gerencia que tiene por objeto salvaguardar y preservar los bienes de la empresa, evitar desembolsos indebidos de fondos, y ofrecer la seguridad de que no se contraen obligaciones sin autorización.”

El control interno es sumamente importante en las empresas, ya que proporciona el grado de confiabilidad que se requiere para:

• Salvaguardar los activos.

• Asegurar la validez de la información.

• Promover la eficiencia en las operaciones.

• Estimular y asegurar el cumplimiento de las políticas y directrices propuestas por la dirección.

Para el diseño e implantación del sistema de control interno, se cuenta con el apoyo de las siguientes técnicas:

• Ejecución del cuestionario de control.

• Análisis del flujo de transacciones.

• Realización de pruebas de cumplimiento.

• Resultados.

• Medidas de corrección.

Así se puede definir el control interno como el establecimiento de los mecanismos y estándares de control que se establecen en las empresas, a fin de ayudarse en la administración adecuada de sus recursos, en la satisfacción de sus necesidades de seguridad, y protección de los activos institucionales, en la ejecución adecuada de sus funciones, actividades, operaciones y reportes; todo ello para el mejor cumplimiento del objetivo institucional.

Objetivos del control interno

Partiendo de que el **control interno** busca contribuir en la seguridad y protección de los bienes de la empresa, en la obtención de información correcta y oportuna, en la promoción de la eficacia de la operación y en la dirección adecuada de la empresa, se puede establecer que su principal objetivo es la ayuda que proporciona al buen

funcionamiento de la institución y a la protección de su patrimonio. Sin embargo, hace falta una información adecuada para comprobar si se satisfacen esas prioridades.

Además, el control interno también sirve para evaluar el desarrollo correcto de las actividades de las empresas, así como la aceptación y cumplimiento adecuados de las normas y políticas que regulan sus actividades.

Objetivos fundamentales del control interno:

• Establecer la seguridad y protección de los activos de la empresa.

• Promover la confiabilidad, oportunidad y veracidad de los registros, así como de la emisión de la información de la empresa.

• Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.

• Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.

• Implantar los métodos, técnicas y procedimientos que permitan establecer adecuadamente las actividades, tareas y funciones de la empresa.

1.2.2 Clasificación del Control

El proceso de establecimiento de controles se puede clasificar de la siguiente manera:

a) De acuerdo con su objetivo

- Correctivos, son aquellos que cuentan en su estructura con los elementos para medir las desviaciones e informar sobre ellas. Implican la determinación de los desvíos y su informe a quien debe actuar sobre éstos. Los controles correctivos, también, pueden ser retroalimentados (datos del pasado) o prealimentados, por ejemplo: presupuestos, ratios.
- No correctivos, son los que prescinden de la medición e información de los desvíos que se pueden producir, como es el caso de controles de separación por funciones y oposición de intereses.

b) De acuerdo con su marco temporal

- Retroalimentados, pues operan sobre hechos sucedidos. Comparan los resultados ocurridos con los esperados.

- Prealimentados, pues operan sobre eventos futuros (en los procesos industriales se denominan “control anticipante”) y previenen la ocurrencia de resultados indeseados.

c) De acuerdo con su pertenencia al sistema operante,

- De secuencia abierta, donde el grupo de control no pertenece al sistema operante; es independiente del mismo.
- De secuencia cerrada, en el que todos los elementos del control pertenecen al propio sistema operante.

d) Controles relacionados con la administración de una organización.

- Control interno: es el conjunto de reglas y normas de procedimiento que regulan el funcionamiento administrativo de una organización. Tienen el propósito de preservar al patrimonio de la empresa de los posibles errores u omisiones, maniobras fraudulentas o daño intencional que pudieran llegar a afectarla.
- Control presupuestario: es el cotejo periódico de los ingresos y de los gastos reales de un período con el fin de poner en evidencia las desviaciones a lo presupuestado.
- Control de gestión: proceso mediante el cual los directivos se aseguran la obtención de recursos y el empleo eficaz y eficiente de los mismos en el cumplimiento de los objetivos fijados a la organización.

1.3 Definición de Auditoría

Auditoria es un proceso sistemático, que permite mediante la recolección de evidencias, determinar la confiabilidad y calidad de la ejecución de las actividades realizadas, en congruencia a los criterios de auditoria, requisitos, políticas y procedimientos establecidos en la organización, para la toma de decisiones.

Una auditoría es una de las formas en las que se pueden aplicar diferentes métodos y técnicas, con el objetivo de verificar procedimientos, bienes, la labor y beneficios alcanzados por la empresa que solicita la auditoría. La auditoría intenta también brindar pautas que ayuden a los miembros de una empresa a desarrollar adecuadamente sus actividades, evaluándolos, recomendándoles determinadas cosas y revisando detenidamente la labor que cada uno cumple dentro de la organización.

1.4 Tipos de Auditorías

1.4.1. Auditoría Informática:

La auditoría informática es una prueba que se desarrolla con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y metas de una organización.

Para esta prueba existe un conjunto de conocimientos, normas, técnicas y buenas prácticas dedicadas a la evaluación y aseguramiento de la calidad, seguridad, razonabilidad, y disponibilidad de la información tratada y almacenada a través del computador y demás dispositivos, así como de la eficiencia, eficacia y economía con que la administración de la organización está manejando dicha información y todos los recursos físicos y humanos asociados para su adquisición, captura, procesamiento, transmisión, distribución, uso y almacenamiento. Esto en busca de emitir una opinión o juicio, para lo cual se aplican técnicas de auditoria de general aceptación y conocimiento técnico específico.

La Auditoría Informática deberá estar formada no sólo por la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

- **Auditoría de Redes**

Es el análisis llevado a cabo de manera exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, tomando en cuenta, en la evaluación, los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones, accesos privilegios, administración y demás aspectos que impactan en su instalación, administración, funcionamiento y aprovechamiento. Además, también la auditoría de red toma en cuenta la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red.

Esta clase de auditoría ha cobrado una importancia tal, que hoy en día su aplicación es altamente demandada en casi todas las instituciones en donde se realizan auditorías de sistemas.

Con la implementación de una auditoría a los sistemas de redes de cómputo, se busca valorar todos los aspectos que intervienen en la creación, configuración, funcionamiento y aplicación de las redes de cómputo, a fin de analizar la forma en que se comparten y aprovechan en la empresa los recursos informáticos y las funciones de sistemas; también se evalúan la distribución de cargas de trabajo, la centralización de los sistemas de redes computacionales y la repercusión de la seguridad, protección y salvaguarda de información, personal y activos informáticos.

Para realizar una auditoría de la red de una empresa, se propone examinar las siguientes características:

• Los objetivos de una red de cómputo.
• Las características de la red de cómputo.
• Los componentes físicos de una red de cómputo.
• La conectividad y comunicaciones de una red de cómputo.
• Los servicios que proporciona una red de cómputo.
• Los sistemas operativos, lenguajes, programas, paqueterías, utilerías y bibliotecas de la red de cómputo.
• Las configuraciones, topologías, tipos y cobertura de las redes de cómputo.

- **Auditoría del Desarrollo**

El desarrollo de un software debe estar sometido a un exhaustivo control de cada una de sus fases, ya que, en caso contrario, además de que puede elevar los costes, podría generar una total insatisfacción del usuario si finalmente no cumple las funcionalidades necesarias, así como la eficiencia de las interfaces de esta. Además, la auditoría deberá comprobar la seguridad del software desarrollado al objeto de garantizar que el resultado de su ejecución sea exactamente el previsto, y que no interfiere con el resto de las aplicaciones de la empresa.

Una auditoría de Desarrollo pasa por la observación y el análisis de las siguientes etapas:

a) **Examen de las metodologías utilizadas**: Se revisarán estas, de modo que se asegure la versatilidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de estas.

b) Revisión Interna de las Aplicaciones

- **Estudio de Aptitud de la Aplicación**
- **Definición lógica de la Aplicación.** (Se examinará que se han completado los propósitos lógicos de actuación, en función de la metodología elegida y la finalidad del proyecto).
- **Desarrollo Técnico de la Aplicación**. (Se verificará que éste es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deberán ser compatibles entre sí, y a ser posible con las ya existentes en el sistema de la empresa).
- **Diseño de Algoritmos.** (Deberán poseer la máxima sencillez, modularidad y economía de recursos).
- **Metodología de Ensayos.** (Se realizarán de acuerdo con las Normas de la Instalación. Se realizarán juegos de ensayo de datos, sin que se permita en ningún caso el uso de datos reales).
- **Documentación de la Aplicación.** (Cumplirá la Normativa establecida en la Instalación, tanto la de Desarrollo como la de su puesta a Explotación).
- **Recursos Humanos Utilizados**. (Deben fijarse las tareas de análisis puro, de programación y las intermedias para cada elemento que constituye el **grupo** de desarrollo. En Aplicaciones complejas se recomienda variaciones en la composición de este, pero estos deberán estar siempre previstos en la planificación inicial).

c) Satisfacción de usuarios: Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse una pérdida si no sirve a los intereses del usuario que la solicitó, o resulta ergonómicamente insuficiente. La aprobación del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento posterior de la Aplicación.

d) Control de Procesos y Ejecuciones Críticas*:* El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no se corresponde con el programa

fuente que se desarrolló, codificó y probó el grupo de Desarrollo de la Aplicación. Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programas módulo no coincidieran se podría provocar, desde errores de bulto (*bugs*) que producirían graves y altos costes de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial/informativo, etc.

- **Auditoría de Bases de Datos**

La auditoría de bases de datos se trata del análisis de las actividades de seguimiento continuo de los controles que la administración ha establecido dentro de los sistemas de bases de datos y todos sus componentes para obtener una seguridad razonable de la utilización correcta de los datos que son almacenados por los usuarios mediante los sistemas de información. El monitoreo y pruebas a los controles determinan la pertinencia y suficiencia de éstos, logrando así ajustar, eliminar o implementar nuevos controles para corroborar su adecuada utilización.

El objetivo de los controles de las bases de datos es minimizar el riesgo inherente que tiene este valioso recurso. Los datos contenidos en las bases de datos pueden considerarse uno de los activos más importantes que tiene la organización, ellos finalmente producirán la información que necesita la empresa para su funcionamiento día a día o para su planificación estratégica.

Por esta razón, la dirección debe proponer políticas de seguridad, procedimientos de utilización y controles pertinentes, y dichas políticas deberán ser divulgadas en la organización.

- **Auditoría de la Calidad**

La auditoría de la calidad es un proceso mediante el cual, se busca, obtener evidencias de los registros que se emiten en el proceso de calidad, en base a declaraciones de hechos o cualquier información, para evaluarlas de manera práctica, su objetivo es determinar si realmente se están cumpliendo políticas y los procedimientos previamente establecidos.

Una auditoría de calidad tiene como objetivo el mostrar la situación real para aportar confianza y destacar las áreas que pueden afectar adversamente esa confianza.

Objetivos de la auditoría de calidad

- Establecer el cuadro de un proyecto
- Verificar la capacidad de realizar o continuar un trabajo específico.
- Verificar qué elementos aplicables del programa o plan de aseguramiento de la calidad han sido desarrollado y documentados.
- Verificar la adherencia de estos elementos con el programa o plan de aseguramiento de la calidad.

El propósito y la actividad de la auditoría es recoger, examinar y analizar la información necesaria para tomar las decisiones de aprobación

Cuando se identifican los puntos débiles los auditores deberán tomar una actitud positiva y utilizar sus conocimientos y experiencias para hacer recomendaciones constructivas.

- **Auditoría de la Seguridad**

La auditoría de la seguridad es el estudio formado por el análisis y gestión de sistemas para evaluar y corregir las distintas vulnerabilidades que se pueden presentar.

Para realizar una auditoría de la seguridad, se debe realizar una planeación de esta; está se hace mediante los siguientes procedimientos:

- **Identificación del Sistema:** el sistema es toda la empresa en la que se realiza la auditoría, en donde se evalúan a las personas y las aplicaciones para las cuales se utiliza el sistema. Se debe tomar en cuenta las políticas de la empresa, lo cual es esencial para el momento de la evaluación; es esta que pone de manifiesto el tipo de control que se posee. Se identifica el sistema, la distribución de la empresa; es decir la organización de las áreas en el sistema, las tareas que poseen las personas que comprenden el sistema. Lo que se quiere es analizar el modo en el que utilizan el sistema, elaborar una guía que muestre los procedimientos en el manejo de los sistemas, identificar las personas que están autorizadas a la administración de los sistemas informáticos. Esto es posible mediante claves de acceso, de manera que se brinde seguridad en la aplicación.

- **Análisis de procesos y recursos:** consiste en identificar los procesos dependiendo del tamaño del sistema, subprocesos, en base a los flujogramas que determinan el recorrido de los procesos y de la información, esto es manejado por los administradores de la red. Cuando se habla de recursos, se trata de los componentes y dispositivos del sistema y las tareas que realizan estos.
- **Análisis de riesgos y amenazas**: se reconocen los riesgos que se presentan en el sistema, además el riesgo de dispositivos y pérdida de recursos. Los dispositivos corren el riesgo de dañarse, de ser robados, es así como puede ocurrir la pérdida de información, y con ello, la integridad de los datos. Esto ocasiona que las operaciones y procesos que se realizan sean ineficientes. En esta etapa se procura verificar cuales son los errores que existen con el manejo de la información.

  Para identificar estos riesgos, se debe analizar las amenazas que se presentan; luego verificar que amenaza a los equipos, los documentos fuentes y primordialmente los programas de aplicación. Se relacionan los recursos, los riesgos y las amenazas en el ambiente propio de trabajo.
- **Análisis y evaluación de controles:** se debe manejar a los grupos que utilizan los recursos, asignando a cada grupo de acuerdo con los recursos que maneje. Debe haber uno o más controles sobre los recursos, los riesgos y las amenazas. El análisis de los controles procura evidenciar si los controles aplicados que el auditor consideró necesarios brindan la seguridad requerida de los recursos.
- **Informes de la Auditoría y Recomendaciones:** cuando se identifica el tipo de sistema, red, recursos, las aplicaciones, los riesgos, las amenazas; lo siguiente es realizar un informe exaltando las partes débiles que amenazan la seguridad del sistema, la red, los recursos y las aplicaciones.

- **Auditoría a Aplicaciones**

Es la revisión que se dirige a evaluar los métodos y procedimientos de uso de aplicaciones o sistemas de información en una entidad, con el propósito de determinar si su diseño y aplicación son correctos y comprobar el sistema de procesamiento de

información como parte de la evaluación de control interno; con el fin de identificar aspectos susceptibles para mejorar o eliminarse.

Las aplicaciones o sistemas de información son uno de los productos finales que genera la infraestructura de la Tecnología Informática en las organizaciones y por ende son el aspecto de mayor visibilidad desde la perspectiva de negocio.

La importancia de una auditoría de aplicaciones radica en el control, eficiencia y eficacia de los sistemas informáticos.

Objetivos de auditoría de aplicaciones.

1. Emitir opinión sobre el cumplimiento de los objetivos, planes y presupuestos contenidos en el Plan de Sistemas de Información sobre la aplicación a auditar.
2. Evaluar el nivel de satisfacción de los usuarios del sistema, tanto de la línea operativa como de las organizaciones de coordinación y apoyo respecto a la cobertura ofrecida a sus necesidades de información.
3. Emitir opinión sobre la idoneidad del sistema de control de accesos de la aplicación.
4. Verificar el grado de fiabilidad de la información.
5. Llevar a cabo la revisión de los métodos utilizados para el desarrollo del sistema computacional de una empresa
6. Evaluación del Control Interno de las Aplicaciones, el cual debe permitir el diseño de nuevos programas desarrollados a la medida de la empresa.
7. Evaluación de todo sistema computacional, en cuanto a la funcionalidad y objetividad del mismo, dado que este debe ser aprobado por el usuario; quien será el responsable de su mantenimiento y desarrollo.
8. Evaluación de la administración adecuada de las bases de datos, puesto que estas contienen información vital de toda empresa, las cuales deben tener ciertas restricciones de acceso.
9. Aumento de la productividad, toda evaluación debe buscar la objetividad de los sistemas computacionales, y estos a su vez, deben ser productivos y ser capaces de contribuir al aumento de la productividad de las empresas que los utilizan.
10. Evaluar la seguridad de los sistemas, esto con el afán de evitar fraudes que representen pérdidas significativas para la empresa.

11. Evaluación de aspectos técnicos del sistema, mediante una serie de técnicas que el auditor debe diseñar, y dar el alcance necesario, para que su trabajo satisfaga las necesidades de la auditoría.

- **Auditoría Física**

La auditoría física trata sobre el análisis para asegurarse que los equipos informáticos se mantengan dando servicio siempre que se les necesite y de una manera segura.
La seguridad física garantiza la integridad de los activos humanos, lógicos y materiales de toda organización.

- **Auditoría de Sistemas Operativo**

El objetivo de esta auditoría es la de verificar el correcto funcionamiento de los sistemas operativos de la organización y sus procesos de entra/salida. Debe analizar los sistemas y si estos se encuentran actualizados con las últimas versiones, además esta auditoría permite descubrir las posibles incompatibilidades entre otros productos de software.
Revisa las políticas y procedimientos de adquisición y mantenimiento de software de sistemas operativos. Para lo cual el auditor revisa lo siguiente:
Los procedimientos relacionados con la identificación y la selección del software del sistema. Mediante entrevistas a la gerencia, para identificar:

- Los requerimientos de software.
- Las fuentes potenciales de software

Análisis de costo/beneficio del software del sistema:
Consiste en revisar la documentación del análisis costo/beneficio y las alternativas que proponen y determinan si cada alternativa potencial fue evaluada adecuadamente. Esta documentación debe tener por lo menos:

- Costo directo financiado para la compra de software.
- Costo de la modificación necesaria para adaptar el software al ambiente de sistemas de información de la organización (si fuera necesario).
- Los requisitos de equipo para ese software.
- Los requisitos de capacitación asociados con la utilización de ese software.
- Los requisitos de apoyo técnico asociado a ese software.

- Análisis de las facilidades del software para cumplir con los requisitos de procesamiento de información.
- Análisis de la capacidad del software para cumplir con los requisitos de seguridad.
- Análisis de la capacidad del software para cumplir con los requisitos técnicos de la organización.

Instalación del software del sistema operativo:

Consiste en revisar el plan o procedimiento para la prueba del sistema, determinar si las pruebas se realizaron de acuerdo con ese plan y en forma exitosa, de no ser así investigar si todos los problemas se evaluaron y resolvieron antes de la instalación del software.

Mantenimiento del software del sistema operativo:

Consiste en revisar la documentación relacionada con el mantenimiento o upgrade del software y determinar lo siguiente:

- Si los estándares de instalación están de acuerdo con la documentación del mantenimiento del software.
- Si los cambios en el software del sistema están debidamente explicados en cuanto a su motivo y aprobación.
- Si existen pruebas de que el cambio realmente se hizo.
- Si el personal responsable del cambio del software del sistema no pertenece al grupo de programadores.
- Si se proporciona a los usuarios del sistema documentación sobre los cambios que se realizarán.
- Si existe un registro o una bitácora de los cambios realizados al sistema.
- Si existen los controles suficientes para asegurarse que los operadores no podrán hacer cambio al sistema sin asesoría del grupo responsable de la instalación de estos cambios.

Seguridad del software del sistema operativo:

Consiste en revisar los procedimientos para el acceso al software del sistema y a su documentación, para esto se entrevista a la gerencia o personal adecuado, para identificar los procedimientos de seguridad para restringir el acceso al software del sistema así como el personal que tiene acceso al software del sistema y a su documentación.

- **Auditoría de Sistemas en Producción**

La auditoría del sistema de producción es un proceso sistemático que se preocupa de la detección de deficiencias o irregularidades en las que puedan ocurrir en esta área. De esta forma la empresa puede prevenir ciertos riesgos de producción a través de su exhaustiva exanimación y valorización de los procesos y desempeño de esta área; además de constar con una base de información para la toma de decisiones.

La finalidad de la auditoría es ayudar a la dirección a lograr la administración más eficaz logrando la interrelación de todos sus sistemas con un funcionamiento satisfactorios verificando los siguientes puntos:

- Determinar lo adecuado de la organización de la entidad.
- Verificar la existencia de objetivos y planes coherentes y realistas.
- Vigilar la existencia de políticas adecuadas y el cumplimiento de estas.
- Comprobar la confiabilidad de la información y de los controles establecidos.
- Verificar la existencia de métodos o procedimientos adecuados de operación y la eficiencia de estos.
- Comprobar la utilización adecuada de los recursos.

Procedimientos que analizar:

Diseño del sistema

Programación de la producción

Control de calidad

Almacén e inventarios

Productividad técnica y económica

Diseño y desarrollo de productos

Revisión de la planificación de la producción.

Verificación de la logística aplicada al proceso productivo.

Estudios de los procesos productivo.

Revisión de los flujos de procesos.

Control de los tiempos aplicados.

Verificación del control de rendimiento.

Otras Auditorías Informáticas son:

- **Auditoría jurídica informática**

Forma parte fundamental de la auditoría informática, su objetivo es comprobar que la utilización de la informática se ajusta la legislación vigente. Es esencial para evitar posibles reclamaciones de cualquier clase contra el sujeto a auditar. Por ello el trabajo del auditor es la medida preventiva idónea contra sanciones en el orden administrativo o incluso penal, así como indemnizaciones en el orden civil por daños y perjuicios a los afectados.

- **Auditoría a la gestión Informática**

Se enfoca en la revisión de las funciones y el objetivo principal es evaluar actividades de tipo administrativo, a fin del cumplimiento adecuado de la gestión administrativa del sistema, las funciones y operaciones computacionales; también verifica el correcto funcionamiento de las actividades que ayudan a las instalaciones informáticas, programas e información, que estas satisfagan las necesidades de mobiliario, equipos, uso, protección, mantenimiento y demás activos del área de informática de la empresa.
Otro objetivo es el de verificar el cumplimiento de funciones del personal: hacer más eficiente a los empleados y usuarios.

- **Auditoría ergonómica de sistemas computacionales**

Uno de los aspectos menos analizados en el área de sistemas es la afectación que causan el mobiliario y los propios sistemas computacionales en los usuarios de computadoras; estos aspectos pueden llegar a influir en el bienestar, salud y rendimiento de los usuarios, razón por la cual se deben considerar mediante una auditoría especializada.
Este tipo de auditoría se define así:
Revisión técnica, específica y especializada que se realiza para evaluar la calidad, eficiencia y utilidad del entorno hombre-máquina-medio ambiente que rodea el uso de sistemas computacionales en una empresa. Esta revisión se realiza también con el propósito de evaluar la correcta adquisición y uso del mobiliario, equipo y sistemas, a fin de proporcionar el bienestar, confort y comodidad que requieren los usuarios de los sistemas de cómputo de la empresa, así como evaluar la detección de los posibles

problemas y sus repercusiones, y la determinación de las soluciones relacionadas con la salud física y bienestar de los usuarios de los sistemas de la empresa.

CASO PRÁCTICO

Fresco y Murillo, Auditores Informáticos es una Firma local dedicada a la prestación de servicios profesionales que actúa en la ciudad de Panamá. Entre sus clientes se cuentan empresas comerciales, agropecuarias, de servicios financieros, entre otras.

Un día Murillo se encuentra en el Club con un amigo empresario, el Ing. Félix Nomore, quién le comenta que ha fundado la empresa Constructora S.A y que ha escuchado de las auditorías informáticas y que quiere contratar a un auditor externo para que dictaminara, además del personal técnico, contable y administrativo, pero tomando en cuenta que se trata de una empresa familiar en la que los socios se tienen absoluta confianza, y que piensa que los proveedores y clientes no serán difíciles de manejar; se mantiene en duda si es necesario o no realizar este tipo de auditoría en su empresa.

Asuma el papel de Murillo y fundamente la necesidad de la auditoría con base en las disposiciones legales, etc., si existieran, y de conveniencia para la empresa. Piense que potencialmente puede ser un cliente para su Firma.

BIBLIOGRAFÍA:

- Leydi Grimaldo. (2014). LA IMPORTANCIA DE LAS AUDITORIAS INTERNAS Y EXTERNAS DENTRO DE LAS ORGANIZACIONES. Opción de grado. Universidad militar Nueva Granada. Colombia. Recuperado de: http://repository.unimilitar.edu.co:8080/bitstream/10654/13537/1/Importancia%20de%20las%20Auditorias.pdf
- Sandoval, Hugo. (2012). INTRODUCCIÓN A LA AUDITORÍA. Primera edición. ISBN 978-607-733-137-7. Red Tercer Milenio S.C. Mexico. Recuperado en: http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf.
- Villalobos Johnny. (2008). Auditando en las Bases de Datos. Universidad Nacional de Costa Rica. UNICIENCIA 22 pp. 135-140.
- MUÑOZ RAZO, Carlos. (2002). AUDITORÍA EN SISTEMAS COMPUTACIONALES. Prentice Hall

II. Organización de la Función de Auditoría

OBJETIVOS:

- Conocer las características que debe tener un auditor
- Describir la importancia del seguimiento y proceder con ética profesional.

¿DE QUÉ TRATA ESTA SECCIÓN DE APRENDIZAJE?

Este capítulo desarrollará las características de un auditor; la importancia de la existencia de la ética Profesional, la cual cabe resaltar es de vital importancia en los tiempos vigentes, ya que la profesión del auditor conlleva grandes responsabilidades y obligaciones, pues se deposita en ellos la confianza de evaluar y emitir una opinión y a partir de ésta se tomarán numerosas decisiones que generarán cambios dentro de las organizaciones.

Las normas de Auditoria son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de su trabajo. El auditor dentro del desarrollo de su profesión debe conocer la empresa a la cual está revisando, ya que puede estar sujeta y diferentes tipos de normas.

II Organización de la Función de Auditoría

2.1 Normas Generales de Auditoría

La auditoría se rige por normas y criterios, los que son emitidos por asociaciones de profesionales quienes aportan experiencia, conocimientos y actualizaciones en estas áreas, con el objetivo de que los practicantes de la profesión conozcan las normas y las cumplan en el desarrollo de cualquier auditoría.

A continuación, se presentan las normas generales de auditoría emitidas por el AICPA:

Normas generales:

- La auditoría debe ser realizada por personal que cuente con la capacitación técnica adecuada y la competencia para ejercer como auditor.
- El auditor debe conservar una actitud mental independiente en todos los aspectos.
- El auditor debe ser diligente en la presentación de los resultados de su auditoría.

Normas generales para el trabajo:

- Para que una auditoría sea eficiente y eficaz, se debe planear y supervisar cabalmente.
- El control interno se debe entender en estructura y contenido a fin de aplicarlo en la planeación y determinación de la naturaleza, duración, extensión y profundidad de la realización de una auditoría.
- La evidencia que soporta el informe del auditor debe ser suficiente, competente y oportuna, esto se logra mediante las técnicas, métodos y procedimientos de auditoría.

Normas de la información:

- El informe de la auditoría debe presentarse en estricto apego a las normas de auditoría generalmente aceptadas.
- En el informe de la auditoría se deben señalar las observaciones que se hayan detectado durante el periodo de evaluación, destacando aquellas desviaciones de los procedimientos normales de la operación de la empresa y de los principios generalmente aceptados.

2.2 Normas Ético – Morales que Regulan la Actuación del Auditor

2.2.1 Marco Conceptual de la Ética

Se identificarán algunas definiciones y conceptos básicos sobre la ética esenciales del comportamiento humano.

Ética

"Relativo a la ética o moral, o que está de acuerdo con sus principios o su exigencia. Parte de la filosofía que estudia los fundamentos y las normas de la conducta humana**".**

Moral

"Del latín moralis. Ciencia que enseña las reglas que deben seguirse para hacer el bien o evitar mal…"

"Conjunto de principios y reglas que recomiendan lo bueno y rechazan lo malo…"

Social

"Que pertenece a, o se relaciona con las sociedades humanas… Sistema de organización social, política y económica que busca los beneficios de la colectividad y no los de los intereses individuales".

Con el análisis de los anteriores conceptos, vemos que la moral está relacionada con las normas de conducta de carácter social, jurídico, profesional y religioso que regulan la actuación del hombre en la sociedad, de acuerdo con los preceptos que se establecen conjuntamente para servir de guías en el accionar del hombre dentro de la misma sociedad.

Lo mismo ocurre con la actuación del profesional dedicado a la auditoría, ya que éste debe conducirse de acuerdo con las normas de conducta social, moral, religiosa, jurídica y profesional, las cuales regularán su actuación como profesional de la auditoría ante la sociedad, autoridades, empresas y empleados de estas últimas.

Sin embargo, la conceptualización de ética va más allá de estos conceptos, como lo señala Nicola Abbagnano en su diccionario de filosofía que dice:

"La ética es en general la ciencia de la conducta y existen dos concepciones fundamentales de esta ciencia, a saber:

1. La que considera como ciencia del fin, al que debe dirigirse la conducta del hombre y de los medios para lograr tal fin y derivar tanto el fin como los medios de la naturaleza del hombre.

2. La que la considera como la ciencia del impulso de la conducta humana, e intenta determinarlo con vistas a dirigir o disciplinar la conducta misma."

"Estas dos concepciones se han entrelazado en formas diferentes, tanto en la antigüedad como en el mundo moderno la primera, en efecto, habla el lenguaje ideal con el que el hombre se dirige por naturaleza la segunda, en cambio, habla de los motivos y de las causas de la conducta humana, o también de las fuerzas que la determinan y pretenden atenerse al reconocimiento de los hechos." Gutiérrez Sáenz dice que 'la Ética estudia reflexivamente el fundamento de la conducta moral'. Esto quiere decir que el hombre desde el principio de su vida social (socialización) está sujeto todo el tiempo a seguir una serie de reglas, normas o leyes. Se crea entonces en el individuo una conciencia normativa que le indica cuáles son los caminos adecuados que lo conducirán ordenadamente y con la aceptación de sus congéneres a convivir y obtener los logros que se proponga, como son: la felicidad, la perpetuación, la autorrealización y otros más. Además, como señala Larroyo todas las normas se crean en contacto con los otros seres humanos, por lo que esa conciencia normativa es, en rigor, una conciencia social normativa."

Atendiendo a lo anterior, la definición propuesta de ética profesional del auditor es la siguiente:

Es el conjunto de valores y principios éticos, morales y profesionales que permiten regular la actividad del profesional dedicado a la auditoría, con el fin de mejorar su actuación en las empresas que audita, así como establecer la responsabilidad que éste adquiere con el desarrollo de esta profesión.

Sin embargo, la acepción de ética es mucho más amplia, según el autor y la corriente que se tomen en cuenta para su análisis y aplicación. Esta materia pretende regular el comportamiento y los deberes éticos y profesionales del auditor; de esta manera, encontramos que este campo de estudio es demasiado amplio y tiene muchas corrientes de pensamiento y autores, opuestos entre sí, y diversas formas de utilización.

Debido a ello, a continuación, le presentaremos las principales corrientes del pensamiento ético:

Principales corrientes éticas

Debido a que existen muchas corrientes de pensamiento respecto a las doctrinas ético-filosóficas, vamos a seguir las corrientes más características de esta materia aquí es que se mencionan algunas de importancia en el estudio de la ética en la actuación profesional del auditor:

Doctrina ética griega
Doctrina ética aristotélica
Doctrina ética cristiana
Doctrina ética kantiana
Doctrina ética marxista
Doctrina ética existencialista
Doctrina ética pragmática

2.2.2 Principios de Axiología y Valores Éticos

Para poder hablar de los valores del auditor, lo primero es considerar las bases fundamentales de la ciencia que estudia la teoría filosófica de los valores; esto se profundiza mediante la axiología, cuyo significado es:

Axiología se deriva del griego axios, valor y logia (de logos), tratado o teoría, teoría del valor.

“Ciencia de los valores, en especial de los valores morales.”

La axiología entonces es la ciencia que trata de los valores de carácter moral que pretenden normar la conducta de los individuos ante la sociedad; es evidente que el auditor, como parte de una sociedad, debe considerar y acatar los valores ético-morales regulados mediante esta ciencia. Por ello, es necesario profundizar un poco sobre estos valores, antes de proponer las normas éticas que regularán la actuación del auditor.

Aunque la definición de valor es la siguiente: “del latín valor-oris, de valore: valer. Precio, costo o utilidad o valía”, desde el punto de vista filosófico estos conceptos adquieren otro significado, pues desde la antigüedad así se designaban los bienes de la cultura y los bienes vitales o espirituales del individuo, de los cuales no se concebía su existencia

como entes aislados ni autónomos, sino como los atributos indispensables del ser. (Estrada Parra: 1992-1994.)

Según Estrada Parra, cuando cita a Max Scheler, señala que los valores son cualidades del orden material, aunque también son objetos ideales. Esto último fue explicado por Hartmann. Para Aristóteles, la bondad, la belleza, la justicia, la verdad y la santidad son entes que no son reales sino meramente ideales; aunque éstos se han considerado como los principales valores que dan las pautas del valor filosófico que pretende alcanzar el ser.

Las características de los valores son:

Objetividad. Los valores existen en sí y por sí mismos, y no es necesaria su realización para que existan. Son independientes del sujeto que los obedece o destaca.

Dependencia. Aunque los valores tienen existencia propia, están subordinados a la realidad, lo cual permite que el ser humano conozca su existencia. Además, a pesar de su intemporalidad, los valores son parte de la realidad.

Polaridad. El valor siempre se presenta como una forma de perfección, y es una forma antagónica de la imperfección o la carencia. El valor verdadero se opone al falso, la belleza a la fealdad, la bondad a la maldad.

Cualidad. Los valores no están relacionados con la cantidad sino con la cualidad; éstos no existen porque puedan aumentar o disminuir, sino porque el hombre se adecua o se acerca a ellos.

Jerarquía. Los valores se dan en un orden establecido, según su importancia, y este orden se modifica según quien los clasifica.

Para Scheler, los valores son jerarquizados de acuerdo con esta propuesta:

Valores de lo agradable y lo desagradable (jerarquía de grado inferior). Son los que tienen relación inmediata con los sentidos y las sensaciones del placer contra el disgusto.

Valores de lo vital y lo antivital (jerarquía de grado medio inferior). Son aquellos cuya convergencia está encaminada a conservar y ampliar la vida en contra del aniquilamiento. Raúl Gutiérrez Sáenz cita esta jerarquía como valores de lo noble y de lo vulgar.

Valores espirituales y no espirituales (jerarquía de grado superior). Son los que están más allá de los entes físicos, aunque sólo se perciben a través del hombre.

Valores religiosos y profanos (valores de grado superior). Son aquellos que se dan entre la tesis de lo santo y lo profano.

También se puede citar la clasificación propuesta por De Finance, quien agrupa la jerarquía de los valores como sigue:

Valores infrahumanos. Son aquellos que perfeccionan al hombre en sus estratos inferiores: la fuerza, el placer, la salud, la agilidad, etcétera.

Valores humanos inframorales. Aquí se colocan todos los valores humanos:

Valores económicos

Valores no-éticos

Valores estéticos

Valores sociales

Valores morales. Son los valores que dependen exclusivamente del libre albedrío del individuo, en busca de la virtud y el nivel íntimo del comportamiento del individuo. Por ejemplo, entre éstos tenemos: la virtud, la prudencia, la justicia, la fortaleza y la templanza.

Valores religiosos. Considerados como el nivel superior, pues dependen de las potencias superiores al hombre. Por ejemplo, la santidad, la gracia, la caridad, etcétera.

Según el criterio del mismo pensador, analizaremos las características de los valores:

Son cualidades ideales, pues existen en el espacio y en el tiempo, aunque no reales.

Son alógicos, no captables por la razón, sólo se perciben, pero no son lógicos.

Son contenidos a priori, nacen de la comprensión de nuestra propia experiencia a través de la intuición.

Son objetivos, se dan independientemente de que sean conocidos o estimados.

Son trascendentes, como son cualidades ideales, trascienden a los demás.

Son materiales, tienen un contenido concreto que no se reduce a una pura forma o estructura universal, sino que se materializa en la esencia del ser.

Se distinguen respecto al bien, pues mientras el bien puede ser destruido, el valor permanece sin ser destruido.

Principios y valores del auditor

Los siguientes son los aspectos fundamentales que debe poseer el profesional que se quiera dedicar a la actividad de auditoría, a fin de que identifique y cumpla los requerimientos que le marca la sociedad para realizar esta función.

Honestidad: Se dice de quien actúa con veracidad, sinceridad, franqueza, honradez e imparcialidad en el cumplimiento de cualquier encomienda, actividad o trabajo. En el caso del auditor, es el cabal cumplimiento de cada una de estas cualidades, con lo cual proporciona la garantía de calidad profesional y moral que demandan de esta actividad las empresas y personas.

Integridad: La persona que posee esta cualidad es de principios sólidos y fundamentales y actúa en forma honorable, recta, valerosa y se apega a sus convicciones, cualesquiera que éstas sean, y las hace respetar; lo mismo sucede con el cumplimiento de los compromisos, trabajo y actividades que se le encomiendan. Está claro que el profesional que actúa como auditor debe poseer estas cualidades.

Cumplimiento: Se dice que una persona es cumplida y digna de confianza, cuando cumple escrupulosamente sus promesas, sus compromisos y respeta la esencia y letra de los convenios que contrae. El auditor que desea poseer esta cualidad debe actuar conforme se indica en este punto, ya que será lo que le ayudará a realizar cabalmente sus actividades.

Lealtad: Es la cualidad que caracteriza a quien es noble, recto, honesto y honrado con su familia, sus amigos, patrones, clientes y con su país, respetando sobre casi todas las cosas una adhesión y constancia con quienes le unen lazos de amistad, amor o profesionalismo. En el caso del auditor, además del cabal respeto a lo anterior, también se considera que es la fidelidad que guarda para con sus auditados, no utilizando ni revelando información que obtiene en forma confidencial de la empresa que audita. En el contexto profesional, también se entiende como la emisión de juicios independientes, profesionales y apegados a lo que detectó en su evaluación, evitando cualquier influencia indebida y conflicto de intereses.

Imparcialidad: Es cuando una persona, en este caso el auditor, busca actuar de manera equitativa en el cumplimiento de su trabajo o de cualquier acción que emprende, tratando de ser siempre justo, honesto y razonable en los juicios que emite, y evitando, tomar

partido hacia algún lado en cualquier auditoría. Además, como profesional de la auditoría, siempre debe estar dispuesto a reconocer errores y a cambiar de posición, creencia y acciones cuando sea necesario, y debe procurar actuar siempre con un amplio compromiso de justicia, equidad, tolerancia y trato igual con los funcionarios y empleados que audite. Lo mismo se aplica a otros profesionales.

Respeto a los demás: Es la cualidad que caracteriza a quien demuestra consideración y estima por la dignidad, la intimidad y el derecho de autodeterminación de la gente, al actuar siempre de manera cortés, expedita y decente, y al proporcionarles lo que necesitan para la mejor toma de decisiones, sin avergonzarles ni degradarles. Esto es lo que debe hacer el auditor, independientemente del puesto y posición que representa para las empresas.

Ciudadano responsable: Se dice de la persona, en este caso del auditor, que está dispuesta a respetar y hacer cumplir las leyes, normas y reglamentos del país, al aceptar la responsabilidad y solidaridad, tanto en los derechos como en las obligaciones, que le imponen la sociedad, las empresas y sus conciudadanos. Esta persona respeta los principios y reglas que regulan las relaciones laborales, morales, comerciales, sociales y de cualquier otro tipo; también evita y, en su caso, protesta contra las injusticias.

2.2.3 Criterios y Responsabilidades del Auditor

Responsabilidad hacia la sociedad:

- Esta responsabilidad se refiere a la independencia del criterio, es decir, que al expresar cualquier juicio profesional el auditor aceptará la obligación de sostener un criterio libre e imparcial.
- Calidad profesional de los trabajos realizados: Con relación a la prestación de cualquier tipo de servicio se deberá considerar que la opinión del auditor deberá estar adecuada y actualizada conforme a las disposiciones legales aplicables.
- Preparación del Auditor: El auditor que preste sus servicios deberá tener la capacidad necesaria para efectuarlos, es decir no basta con que concluya solamente un grado de estudios, como lo es en este caso la licenciatura si no que para poder tener un panorama amplio que le permita auditar deberá de contar con una especialidad aunada a la experiencia profesional

- Responsabilidad Personal: El auditor deberá aceptar la responsabilidad que adquiere y el compromiso que tiene para con la organización y la obligación de concluir su trabajo.

Responsabilidades en relación con su equipo de trabajo:

- Secreto Profesional: El auditor al momento de aceptar el trabajo adquiere la obligación de guardar secreto profesional y por ningún motivo revelar información de los hechos, datos o circunstancias de las cuales tenga conocimiento con motivo del trabajo de auditoria solicitado a menos que los interesados lo autoricen.
- Rechazo de tareas que no cumplan con el código de ética: El auditor tendrá la obligación de conservar en cualquier momento su honor y dignidad profesional bajo el entendido de que no podrá por ningún motivo aceptar propuesta alguna relacionada con arreglo o asunto que no cumpla con la moral que comprende este código y que por ende sea contraria a los lineamientos aplicables por ley o que en su defecto esta conducta pudiera constituir un delito.
- Lealtad hacia la organización o empresa: El auditor mientras desempeñe sus funciones no podrá realizar alguna práctica que llegue a perjudicar a la empresa quien contrate sus servicios.
- Retribución Económica: Es importante mencionar que el auditor tiene derecho por los servicios prestados a recibir una retribución económica justa conforme al trabajo realizado

Responsabilidad hacia la profesión:

- Respeto a los colegas y a la profesión: El auditor deberá cuidar las relaciones con los colaboradores que integran su equipo de trabajo y con los miembros de la organización o empresa que le ha solicitado el trabajo de auditoria, siempre deberá buscar la dignidad de la profesión.
- Dignificación de la imagen a base de calidad: El auditor deberá en todo momento dignificar la profesión ofreciendo una calidad profesional y personal, creando una imagen positiva y de respeto por parte de la organización.
- Difusión y Enseñanza de los conocimientos: El auditor deberá difundir sus conocimientos a miembros de la organización, colegas y colaboradores, a su vez deberá siempre vigilar que toda la información proporcionada esté debidamente

fundamentada esto es que se establezcan y se remita a las disposiciones legales y las fuentes de información en las cuales se basa su opinión y en algunos casos la obligatoriedad de la misma.

2.2.4 Normas Profesionales del Auditor

Dentro de un plano netamente laboral, el auditor también debe cumplir con ciertos criterios y obligaciones que regulan su actuación como profesional de esta materia, acatándolos de acuerdo con su nivel de participación en la auditoría, con su rango de autoridad y con la responsabilidad que adquiere al ser contratado por una institución.

Cumplir con los planes, programas, contratos y presupuestos acordados:

Sin importar que el auditor sea empleado de la empresa auditada o que sea independiente, es su obligación cumplir y respetar los planes, presupuestos y programas de trabajo que le sean asignados para realizar su labor.

Es su obligación saber respetar y hacer cumplir las indicaciones recibidas como subordinado, o las concertadas en caso de ser un auditor independiente.

Aplicar los métodos, técnicas y procedimientos de evaluación debidamente avalados:

Como profesional de la auditoría, ya sea subordinado o independiente, el auditor debe saber aplicar una serie de métodos, procedimientos, herramientas, técnicas y guías de evaluación que le permitirán obtener resultados acertados en cualquier revisión que realice, siempre y cuando estas herramientas hayan sido previamente diseñadas, ya que ello le permitirá realizar su trabajo con eficiencia y eficacia. Además, contar con el diseño previo de tales herramientas y utilizarlas correctamente, aunado a sus conocimientos y experiencia en otras auditorías, le ayudará a obtener los mejores resultados en la evaluación.

También diremos que es obligación del auditor utilizar estas herramientas en la realización de una auditoría.

Revisar y profundizar sobre los puntos relevantes de las áreas que serán auditadas:

De acuerdo con los planes y programas de auditoría, el auditor debe hacer una profunda revisión de todos los aspectos que considere relevantes en las áreas y actividades que vaya a evaluar, ya sea porque ha elegido previamente algunos puntos específicos para analizarlos, o simple y sencillamente porque, como resultado de alguna evaluación preliminar, necesita verificar con más detalle algunos de los aspectos importantes de dichas áreas.

Es necesario reiterar que no es elección del auditor profundizar en los aspectos relevantes, es su obligación; también es su obligación revisar aquellos que supuestamente no son importantes.

Elaborar las evaluaciones, dictámenes e informes conforme a las normas y lineamientos que regulan el desarrollo de las auditorías:

Ya hemos destacado, en los aspectos ético-moral y profesional-personal, la importancia que tiene que el auditor cumpla con los criterios y obligaciones establecidos en cuanto a la forma de realizar su evaluación y la manera de emitir su dictamen, destacando que su emisión está regulada por leyes, asociaciones y por el propio auditor. Entonces, podemos decir que en los criterios y responsabilidades en el aspecto laboral del auditor debe ocurrir lo mismo, ya que también es su obligación profesional, laboral y ética apegarse a las normas y lineamientos que regulen el desarrollo de una auditoría.

Esto, a la vez que es una obligación, es una garantía para el auditado, en el sentido de que el auditor siempre utilizará los mismos criterios en su evaluación y emisión de informes.

Esto es lo que da el soporte necesario para confiar en que el trabajo del auditor se desarrolla eficientemente.

Acatar las normas disciplinarias y de conducta de la empresa de auditoría externa, así como las de la empresa auditada:

Los criterios, normas, condiciones, obligaciones y reglamentos establecidos dentro la empresa auditada tienen que ser estrictamente respetados, tanto por el auditor que realiza la auditoría como por cada uno de sus colaboradores y por el personal que es auditado, ya que éstas son las normas de conducta que regularán invariablemente las

actividades, funciones y obligaciones entre este profesional y la institución, no sólo en el aspecto laboral, sino también en el disciplinario.

Un auditor nunca debe romper las normas de conducta y medidas disciplinarias establecidas en la institución auditada; siempre deberá acatarlas.

Capacitar y adiestrar al personal subalterno:

A la vez que es una obligación laboral, también es conveniente capacitar constantemente a los auditores, tanto para provecho del auditor como para beneficio de la empresa que lo contrata; es decir, es una exigencia profesional y moral proporcionar la capacitación necesaria a los auditores, a fin de que éstos se desempeñen óptimamente en su trabajo. Entre más preparado y profesional sea el personal que realiza una auditoría, más eficientes y confiables serán los resultados de las evaluaciones.

Además, con la capacitación de los auditores se contribuye a la mayor eficiencia y eficacia en la realización de este tipo de trabajos, ya que esto no sólo ayuda a solventar la responsabilidad patronal ante los trabajadores, sino que al mismo patrón le permite tener una mayor competitividad en el ejercicio de esta profesión, lo cual es muy provechoso ya que puede contar con personal altamente capacitado para cumplir con las actividades tan especializadas que demanda esta profesión. Igual o mayor beneficio obtiene quien actúa como jefe, ya que así será más descansada la conducción del trabajo, debido a que puede contar con auditores capacitados. Otra razón para capacitar a los auditores es que esto beneficia profesionalmente a las empresas auditadas, ya que entre más capacitado esté el auditor, la revisión que realice será más profesional, más profunda y con mayor competencia, lo cual es una garantía de calidad.

2.3 Estructura de Organización de las Empresas y Áreas dedicadas a la Auditoría

Tomando en cuenta que existen muchas empresas y profesionales que se dedican a la auditoría, y debido a las propias características de esas empresas y/o áreas de auditores, a continuación, se presenta una serie de propuestas de organización, bajo las cuales se puede clasificar la estructura de organización de las empresas y áreas de auditoría. Dichas propuestas se dividen en dos grupos.

El primero está determinado por las estructuras de aquellas empresas que se dedican a la auditoría externa. Estas estructuras se agrupan en tres grandes clasificaciones, según

el tamaño de la empresa; claro está, todo será considerado de acuerdo con el número de sus ocupantes y actividades que deban realizar.

Para el segundo caso, la estructura de organización está considerada para aquellas empresas que cuentan con áreas de auditoría interna; en esta estructuración también se ubican tres tipos de áreas de auditoría interna dentro de las empresas, tomando en cuenta el tamaño de la institución y el número de empleados que haya en el área de auditoría interna.

Estructuras de organización de las empresas dedicadas a la auditoría externa:

Para la presentación de esta clasificación de niveles ideales de estructuras de las empresas dedicadas a la auditoría externa, tomaremos el siguiente criterio de agrupación: grandes empresas dedicadas a la auditoría, despachos o empresas medianas dedicadas a la auditoría y pequeños despachos o auditores independientes. Sobre esta base se proponen estos niveles de puestos para adecuarse a las necesidades de la empresa auditora:

Grandes empresas dedicadas a la auditoría:

• Director o gerente general (al nivel de mando superior)
• Funcionarios de cuenta (por empresa o por área de atención)
• Gerentes o jefes de departamento o de área de atención
• Supervisores de auditoría
• Jefes de grupo o responsables de auditoría (Auditores Senior)
• Auditores asignados (Auditores Junior)
• Apoyo administrativo y secretarial

Despachos o empresas medianas dedicadas a la auditoría:

• Gerente de auditoría
• Encargado de auditoría (Auditor Senior)
• Auditores Junior
• Apoyo secretarial

Pequeños despachos o auditores independientes:

• Auditor Senior
• Auditor Junior

• Apoyo secretarial

Es necesario volver a destacar que los niveles de estructura aquí propuestos son indicativos para la organización de cualquier empresa dedicada a la auditoría externa, en la condición de que esta estructuración puede adecuarse a las necesidades concretas de la propia institución, atendiendo los requerimientos de sus áreas, la especialidad de su personal, las necesidades de sus clientes o de cualquier otro tipo de criterio que le ayude a bien evaluar sus funciones, actividades u operaciones, según sus características y necesidades.

Estructuras de organización de las áreas de auditoría interna:

De acuerdo con la estructura de organización, el tamaño de la empresa, las políticas y estilos de dirección de cada institución, la ubicación ideal de las áreas de auditoría interna tiene que ser a nivel de staff o asesoría, dependiendo y reportando directamente a los niveles de mayor jerarquía en la empresa, con subordinación de la dirección general o de una sola de las áreas de alta dirección. Es recomendable, de acuerdo con la estructura de organización de cada empresa, que el área de supeditación sea la administrativa, de contraloría o alguna similar en sus funciones. Sin embargo, nada impide que se pueda depender de cualquier otra área, siempre que sea del ámbito de alta dirección.

Éstas se ubican en los siguientes cinco grupos, de acuerdo con su tamaño: macroempresas, empresas grandes, empresas medianas, empresas pequeñas y microempresas.

Para auditorías internas de macroempresas y empresas grandes:

• Director o gerente al nivel de área funcional
• Gerentes o jefes de departamento, de área o de función a auditar
• Jefes de grupo o encargados (Auditores Senior)
• Auditores internos (Auditores Junior)
• Apoyo administrativo y secretarial

Para auditorías internas de empresas medianas:

• Gerente de auditoría
• Auditor Senior
• Auditores Junior

• Apoyo secretarial

Para auditorías internas de empresas pequeñas y microempresas:

• Auditor Senior

• Auditor Junior

• Apoyo secretarial

También conviene aclarar que la propuesta de niveles de organización de auditoría interna puede ser modificada de acuerdo con las necesidades y características de la institución, a los requerimientos de atención de sus áreas, a su tamaño, giro y actividades, o por cualquier otro tipo de criterio que le permita hacer una evaluación adecuadamente.

CASOS PRÁCTICOS

1. En su empresa se están planteando la posibilidad de realizar una auditoría informática externa contratando personal ajeno que garantice la independencia de los análisis y resultados. El primer auditor candidato a ser contratado no ha delimitado los posibles objetivos y el alcance de la auditoria a realizar y les está ofreciendo las tareas de auditoría a unos precios demasiado reducidos en relación con los precios del mercado. ¿Contrataría a este auditor? ¿Por qué? ¿Incumple algún principio establecido dentro de las normas del auditor?

Solución

No es recomendable contratar a este auditor porque no cumple por completo las normas del auditor.

Incumple los principios al no definir claramente el alcance de la auditoría y de respeto hacia otros compañeros de la misma profesión al ofrecer precios demasiados reducidos respecto a los normales del sector.

Siempre será conveniente contratar a un auditor que cumpla perfectamente con los principios éticos y morales del código del auditor, que proporcione una garantía de la calidad de la auditoría.

2. Marta Casabianca es gerente general de Nutricia SRL, una compañía dedicada a la fabricación de alimentos balanceados para aves. Marta pide a su amiga, la CP Gloria Smith, que haga una auditoría de los estados contables de la Compañía al 31/12/x1 en dos semanas pues debe entregar esos estados contables auditados al Banco Local, quién los requiere para evaluar el otorgamiento de un préstamo a Nutricia SRL. Marta convino en pagarle a Gloria un honorario fijo más una bonificación si el Banco otorgaba el préstamo. Gloria aceptó el compromiso en los términos propuestos.

Seguidamente Gloria contrató dos estudiantes de la carrera de contador público en la facultad local y dedicó varias horas a explicarles lo que deberían hacer. Concretamente les pidió que revisaran la precisión matemática de los registros contables, los pases al libro mayor y su concordancia con el balance de comprobación que le había suministrado Marta y finalmente que preparan un borrador de los estados contables de publicación.

Dos semanas después, los estudiantes entregaron a Gloria los estados contables finales sin las notas complementarias correspondientes. Gloria revisó esos estados contables y preparó un informe de auditoría con una opinión favorable sin salvedades. No hizo ninguna referencia a las NCP ni a su aplicación uniforme con respecto al año precedente.

Se solicita que:

Con base en los conocimientos de las normas de auditoría que usted pudo obtener de la lectura de este capítulo, evalúe qué acciones de Gloria Smith contradicen las normas de auditoría.

BIBLIOGRAFÍA:

- MUÑOZ RAZO, Carlos. (2002). AUDITORÍA EN SISTEMAS COMPUTACIONALES. Prentice Hall.
- Sandoval, Hugo. (2012). INTRODUCCIÓN A LA AUDITORÍA. Primera edición. ISBN 978-607-733-137-7. Red Tercer Milenio S.C. México. Recuperado en: http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf.
- Heredero C, López J, Romo S, Medina S. (2011). Organización y Transformación de los Sistemas de Información en la Empresa. Esic Editorial. España.

III. Metodología para Realizar Auditorías

OBJETIVOS:

- Proponer una metodología específica que puede ser aplicable a la realización de cualquier tipo de auditoría.
- Aplicar técnicas de selección y evaluación de información para el correcto desarrollo de una auditoría.

¿DE QUÉ SE TRATA ESTA SECCIÓN DE APRENDIZAJE?

Cualquier actividad, requiere de pasos a seguir o procedimientos, así como un doctor debe seguir ciertos pasos, como anestesiar, verificar los signos vitales, para proceder a operar, un auditor, debe seguir ciertos pasos para lograr su objetivo.

Dichos pasos deben cumplirse, no forzosamente uno tras el otro como se muestran en la unidad.

Proponer una metodología específica que puede ser aplicable a la realización de cualquier tipo de auditoría en el campo de los sistemas computacionales, con el propósito de mostrar una forma concreta de llevar a cabo la planeación, selección de herramientas, desarrollo y presentación de los resultados de estas auditorías, para que el lector pueda adoptar esta metodología y en su caso adaptarla a las necesidades concretas de revisión en su ambiente de sistemas.

III. Metodología para Realizar Auditorias

3.1 Marco Conceptual de la Metodología

El primer paso para entender la metodología es identificar el marco teórico sobre el cual se fundamentan los conceptos:

Método:

"Del griego: **methodos,** de meta, con y **odos**, vía.

"Procedimiento, técnica, teoría, tratamiento, sistema".

"Modo de realizar las cosas con orden".

"Procedimiento para hallar el conocimiento y enseñarlo".

Metodología:

"Del griego **Methodos**, método, y **Logos**, tratado.

"Estudio de los métodos que se siguen en una investigación, un conocimiento o una interpretación."

"Descripción secuencial de la manera de efectuar una operación o serie de operaciones."

Planeación:

"Es el proceso de decidir de antemano qué se hará y de qué manera. Incluye determinar las misiones globales, identificar resultados claves y fijar objetivos específicos,

Metodología para realizar auditorías

Con el propósito de interpretar adecuadamente la aplicación de la metodología para realizar auditorías, a continuación, se presenta, en forma genérica, todos aquellos pasos que se deben considerar en la planeación de la evaluación.

1ª etapa: **Planeación de la auditoría**

P.1 Identificar el origen de la auditoría

P.2 Realizar una visita preliminar al área que será evaluada

P.3 Establecer los objetivos de la auditoría

P.4 Determinar los puntos que serán evaluados en la auditoría

P.5 Elaborar planes, programas y presupuestos para realizar la auditoría

P.6 Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría

P.7 Asignar los recursos y para la auditoría.

2ª etapa: Ejecución de la auditoría de sistemas computacionales

E.1 Realizar las acciones programadas para la auditoría

E.2 Aplicar los instrumentos y herramientas para la auditoría

E.3 Identificar y elaborar los documentos de desviaciones encontradas

E.4 Elaborar el dictamen preliminar y presentarlo a discusión

E.5 Integrar el legajo de papeles de trabajo de la auditoría

3ª etapa: Dictamen de la auditoría de sistemas computacionales

D.1 Analizar la información y elaborar un informe de situaciones detectadas

D.2 Elaborar el dictamen final

D.3 Presentar el informe de auditoría

3.2 Planeación de la Auditoría

Los diferentes sistemas de organización, control, contabilidad y en general, los detalles de operación de los negocios, hacen imposible establecer algún sistema rígido de prueba, por lo que el auditor deberá, aplicando su criterio profesional, decidir cuál técnica o procedimiento de auditoria, o conjunto de ellos, serán aplicables en cada caso para obtener la certeza que fundamente su opinión objetiva o profesional. El auditor deberá previa su investigación, documentar todos aquellos aspectos importantes de la auditoria los cuales proporcionarán la evidencia de que ésta se llevó a cabo conforme a las normas aplicables. Esta documentación deberá estar integrada por papeles de trabajo preparados por el auditor y aquellos que le fueran suministrados por la organización auditada o por terceras personas que tenga que conservar para soportar el trabajo realizado. Los papeles de trabajo constituirán la prueba plena del trabajo realizado por el auditor, ya que fundamentan la opinión o informe realizado, constituyen una fuente de aclaraciones o ampliaciones de información siendo la única prueba que tiene el auditor respecto a la solidez y calidad de su trabajo. Esta documentación proveerá la evidencia de la naturaleza y extensión en las técnicas y procedimientos de auditoria siendo la prueba del cuidado y la diligencia con la que el auditor realizó su examen. A su vez consignarán los conocimientos del auditor respecto del área auditada, así como su

habilidad para analizar problemas e identificar situaciones relevantes, reflejando los hábitos de orden, limpieza, visión e ingenio del auditor para realizar su trabajo.

Constituirán el medio más importante a través del cual se lleva a cabo el proceso de supervisión de la auditoria en sus diferentes niveles, sirviendo para calificar la calidad de la planeación de la auditoria el avance entre los tiempos estimados y reales de ejecución atendiendo a la calidad de los resultados. Estos constituirán una fuente básica de información para la conformación, preparación y soporte del informe o dictamen de la auditoria.

La información que debe de contener estos papeles deberá de estar en función a los objetivos que se persigan en la auditoria, estos deberán de establecer claramente las fechas y las fuentes de consulta que se obtuvieron con el propósito de concluir un dictamen.

El auditor establecerá una estrategia global de auditoría que determine el alcance, el momento de realización y la dirección de la auditoría, y que guíe el desarrollo del plan de auditoría.

Para establecer la estrategia global de auditoría, el auditor:

(a) identificará las características del encargo que definen su alcance;

(b) determinará los objetivos del encargo en relación con los informes a emitir con el fin de planificar el momento de realización de la auditoría y la naturaleza de las comunicaciones requeridas;

(c) considerará los factores que, según el juicio profesional del auditor, sean significativos para la dirección de las tareas del equipo del encargo;

(d) considerará los resultados de las actividades preliminares del encargo y, en su caso, si es relevante el conocimiento obtenido en otros encargos realizados para la entidad por el socio del encargo; y

(e) determinará la naturaleza, el momento de empleo y la extensión de los recursos necesarios para realizar el encargo.

3.3 Ejecución de la Auditoría

En esta etapa el objetivo es poder obtener y analizar toda la información del proceso que se está auditando, para así poder obtener toda la evidencia necesaria, competente, suficiente y relevante, para que en el momento de presentar sus conclusiones se encuentren bien fundamentadas, por ello se deben tener en cuenta los siguientes elementos:

- La Pruebas de Auditoria
- Técnicas de Muestreo
- Evidencias de Auditoria
- Papeles de Trabajo
- Hallazgo de Auditoria

El auditor ejecutará el plan de auditoría, el cual incluirá una descripción de:

(a) la naturaleza, el momento de realización y la extensión de los procedimientos planificados para la valoración del riesgo.

(b) la naturaleza, el momento de realización y la extensión de procedimientos de auditoría posteriores planificados relativos a las afirmaciones,

(c) otros procedimientos de auditoría planificados cuya realización se requiere para que el encargo se desarrolle.

El auditor actualizará y cambiará cuando sea necesario en el transcurso de la auditoría la estrategia global de auditoría y el plan de auditoría.

3.4 Dictamen de la Auditoría

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto, la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al dictamen final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Estructura del dictamen final:

- El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción de este.

- Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente.
- Definición de objetivos y alcance de la auditoría.
- Enumeración de temas considerados:
- Cuerpo expositivo: para cada tema, se seguirá el siguiente orden a saber: Situación actual: cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real
- Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- Puntos débiles y amenazas.
- Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
- Redacción posterior de la Carta de Introducción o Presentación.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes.
- Calidad y seguridad de la información y auditoría informática

El Informe debe consolidar los hechos que se describen en el mismo. El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados.

La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

1. El hecho debe poder ser sometido a cambios.

2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.

3. No deben existir alternativas viables que superen al cambio propuesto.

4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

El dictamen es el informe realizado una vez se tiene el resultado de la información, investigación y el análisis efectuado por el auditor, en donde presenta de una manera formal su opinión sobre el área, proceso o actividad auditado, con respecto a los objetivos establecidos, señalando así, las debilidades encontradas, si existen, las recomendaciones que ayuden a eliminar las causas de estas falencias y promover las acciones correctivas necesarias.

Recordemos que las personas auditadas durante el desarrollo de la auditoria deben estar siendo informadas de los hallazgos encontrados, por lo anterior pueden tener acceso a cualquier documentación relativa a algún hecho encontrado.

El informe debe ser presentado de una forma clara, sencilla, tendiendo a ser constructivo y oportuno.

EJERCICIO PRÁCTICO:

En grupos de trabajo, busque en la web un informe de auditoría (en el área informática) de una empresa.

Léalo y analícelo atentamente,

Una vez en clase discuta con los demás grupos:

¿Cuál es el rol de auditor de acuerdo con lo expresado en el informe?

¿Cuál es el rol de la dirección de acuerdo con lo expresado en el informe?

¿Cuál es el párrafo central del informe y qué expresa este?

¿Se dieron o no recomendaciones?

BIBLIOGRAFÍA:

- MUÑOZ RAZO, Carlos. (2002). AUDITORÍA EN SISTEMAS COMPUTACIONALES. Prentice Hall.
- Fundación Eca Global. El Auditor de Calidad. Editorial Fundación Confemetal. Madrid.
- Sandoval, Hugo. (2012). INTRODUCCIÓN A LA AUDITORÍA. Primera edición. ISBN 978-607-733-137-7. Red Tercer Milenio S.C. Mexico. Recuperado en: http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf.
- Leydi Grimaldo. (2014) Auditorías internas y externas en las organizaciones. Universidad Militar Nueva Granada. Colombia.

.

IV. Técnicas de Evaluación Aplicables en Auditoría

OBJETIVOS:

- Identificar los principales instrumentos, técnicas, herramientas y métodos utilizados en la recopilación de información útil para realizar una auditoría.
- Poner en práctica las técnicas de recopilación de información para evaluar la situación de una organización en materia de funcionamiento.

¿DE QUÉ SE TRATA ESTA SECCIÓN DE APRENDIZAJE?

Este capítulo fundamenta las herramientas y métodos tradicionales de recopilación de información de las auditorías tradicionales; también utilizados en el análisis y diseño de sistemas, y las ciencias sociales, a fin de conocer su forma de aplicación y funcionamiento en las auditorías de sistemas computacionales y adaptarlos a las necesidades específicas del ambiente de sistemas que se requiere auditar.

IV. Técnicas de Evaluación Aplicables en Auditoria

4.1 El Examen

En una auditoría, el examen consiste en analizar y poner a prueba la calidad y el cumplimiento de las funciones, actividades y operaciones que se realizan cotidianamente en una empresa, y se aplica en un área o actividad específica o en una unidad administrativa completa. El examen también se utiliza para evaluar los registros, planes, presupuestos, programas, controles y todos los demás aspectos que afectan la administración y control de una empresa o de las áreas que la integran.

El auditor aplica esta herramienta con el propósito de investigar algún hecho, comprobar alguna cosa, verificar la forma de realizar un proceso, evaluar la aplicación de las técnicas, métodos y procedimientos de trabajo, verificar el resultado de una transacción, comprobar la operación correcta de un sistema computacional y para evaluar muchos otros aspectos.

Dentro del ambiente de la auditoría informática, esta herramienta se utiliza, entre muchas cosas, para inspeccionar la operación correcta del sistema, analizar el desarrollo adecuado de los proyectos informáticos, examinar la forma en que se realiza la captura y el procesamiento de datos, así como la emisión de resultados; también se emplea para inspeccionar las medidas de seguridad del sistema y del área de informática, examinar el acceso a dicha área, al sistema, a sus programas y a la información de las bases de datos, para examinar la forma en que se archivan y protegen los datos de los sistemas, sus programas y la propia información; además pone a prueba el cumplimiento de las funciones y actividades de los funcionarios, personal y usuarios del centro de cómputo.

4.2 La Inspección

Es la verificación física de las cosas materiales en las que se tradujeron las operaciones, se aplica a las cuentas cuyos saldos tienen una representación material. (efectivos, mercancías, bienes, etc.).

El término inspección, aplicado al ambiente de sistemas computacionales, también puede ser sinónimo de supervisión, ya que en ambos casos se trata de examinar la forma en que se desarrollan las actividades de un área de sistemas computacionales, a fin de evaluar y emitir un informe sobre el desarrollo normal de sus funciones y operaciones.

La inspección también tiene como propósito monitorear el desarrollo cotidiano de las funciones, actividades y operaciones normales de la empresa, para evaluar y, si es necesario, corregir su desarrollo; claro está, con las diferencias específicas que existen en cuanto a la acepción del vocablo y su aplicación concreta en el ambiente de sistemas. Por ello, es importante tomar en cuenta que no es lo mismo hacer una inspección de auditoría que hacer la supervisión de las actividades de los sistemas.

Esta herramienta se aplica de acuerdo con las características específicas de cada centro de cómputo o de cada sistema computacional. Sin embargo, a continuación, se presentan algunos ejemplos de los posibles aspectos del ambiente de sistemas computacionales en donde se puede aplicar la inspección:

• La inspección de los sistemas de seguridad y protección de las instalaciones, equipos, personal y de los propios sistemas de procesamiento, con el propósito de dictaminar sobre su eficiencia y confiabilidad.

• La inspección de los formatos para la captura de datos y sus procedimientos en su introducción al sistema de procesamiento de información, a fin de evaluar su eficiencia, oportunidad, confiabilidad y veracidad.

• La inspección del uso, almacenamiento y protección de los sistemas, programas e información que se procesa en el centro de cómputo, con el propósito de emitir un dictamen sobre su seguridad y uso.

• La inspección del cumplimiento de las funciones, actividades y responsabilidades de cada uno de los funcionarios, personal, usuarios, asesores y proveedores del área de sistemas, a fin de opinar sobre su actuación.

• La inspección de la distribución geográfica del mobiliario, equipos, sistemas y conexiones del área de sistemas computacionales, así como de los aspectos relativos a su ambiente, ergonomía, funcionalidad, y seguridad.

• La inspección del uso, funcionalidad, configuración y aprovechamiento de las redes de cómputo, así como de sus sistemas operativos, de aplicaciones, desarrollo de sistemas, arquitectura, conexiones y de todos los demás aspectos relacionados con la operación de la red de cómputo.

4.3 Confirmación

Es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operación, en la que participo y por la cual está en condiciones de informar válidamente sobre ella.

Uno de los aspectos fundamentales para la credibilidad de una auditoría es la confirmación de los hechos y la certificación de los datos obtenidos durante la revisión, ya que el resultado final de una auditoría es la emisión de un dictamen en el que el auditor vierte sus opiniones; pero, para que el dictamen sea plenamente aceptado, es necesario que los datos sean veraces y confiables, y que las técnicas y métodos utilizados para la auditoría sean los adecuados.

Un auditor jamás puede fundamentar sus opiniones en suposiciones y conjeturas falsas, ni emitir juicios basados en datos que no sean verídicos o que no estén certificados plenamente, o en datos obtenidos con técnicas y herramientas de auditoría que no garanticen la comprobación de la información recabada.

La absoluta confianza en las opiniones emitidas en el dictamen de la auditoría es uno de los aspectos fundamentales de esta disciplina, debido a que los resultados deben estar fundamentados en información que sea plenamente comprobada y confirmada a través del uso de las técnicas, herramientas, procedimientos e instrumentos adecuados para la auditoría.

La característica fundamental de una auditoría, cualquiera que sea su tipo, es la autenticidad con la que el auditor emite sus opiniones, sean a favor o en contra.

Debemos reiterar que, en la auditoría de sistemas computacionales, al igual que en otras auditorías, la confirmación es uno de los elementos fundamentales que ayudan al auditor a certificar la validez de su dictamen de auditoría.

Como podemos ver, en una auditoría de sistemas computacionales es muy importante comprobar la veracidad y confiabilidad de los datos obtenidos durante la revisión, así como confirmar que los procedimientos utilizados para su captura y procesamiento estén apoyados en pruebas realizadas por el auditor.

De esta manera, el dictamen lleva implícitas la autenticidad y confiabilidad de las pruebas con las que se obtuvo la información; esto por sí solo sería la confirmación de que la información obtenida es veraz, confiable y que está debidamente comprobada.

A continuación, se presentan algunos ejemplos sobre la confirmación en la auditoría de sistemas:

• Confirmar la oportunidad, confiabilidad y veracidad de los pagos de nómina del personal de la empresa, comparando los resultados de una quincena con los cálculos manuales de esa misma quincena.

• Autentificar la captura de una base de datos de los registros de alumnos de licenciatura del plantel sur de una universidad privada, cotejando los registros individuales de esos estudiantes, contra la información emitida en el sistema computacional.

• Validar las desviaciones encontradas en el procesamiento de datos de un lote de captura para ingresar suscriptores de una revista cualquiera para el mes de marzo, a través del cotejo manual de los datos de los suscriptores contra los listados capturados.

• Revisar las licencias del software instalado en los sistemas computacionales de la empresa, a fin de confirmar que no haya software instalado sin licencia.

• Realizar los simulacros de las medidas preventivas y correctivas establecidas en los planes de contingencias del área de sistemas, a fin de confirmar la suficiencia y buen funcionamiento en la aplicación de dichos planes.

• Confirmar la confiabilidad de las protecciones, contraseñas y demás medidas de seguridad establecidas para el acceso a la información y a los sistemas de la empresa, verificando su invulnerabilidad y buen funcionamiento.

4.4 Revisión Documental

Una de las herramientas tradicionales y quizá de las más utilizadas en cualquier auditoría es la revisión de los documentos que avalan los registros de operaciones y actividades de una empresa, principalmente en aquellos casos donde la evaluación está enfocada a los aspectos financieros, el registro de los activos de la empresa y a cualquier otro aspecto contable y administrativo. Esta técnica se aplica verificando el registro correcto de datos en documentos formales de la empresa y, con mucha frecuencia, en la emisión de sus resultados financieros. Esta costumbre de revisar los registros es muy socorrida por los contadores en las auditorías de carácter contable, fiscal y financiero, debido a que es un requisito obligatorio evaluar el registro de las operaciones financieras de la empresa, ya que con esos registros se evalúa la elaboración de sus estados de

resultados financieros. Esto se lleva a cabo mediante la revisión y evaluación de los registros realizados en las llamadas pólizas, libros diarios y otros documentos contables. Sin embargo, además de revisar los documentos financieros de la empresa, también se puede revisar el registro de las actividades y operaciones que se plasman en documentos y expedientes formales, con el fin de que el auditor sepa cómo fueron registradas las operaciones, resultados y otros aspectos inherentes al desarrollo de las funciones y actividades normales de la empresa. En esta evaluación se revisan los manuales, instructivos, procedimientos diseñados para las funciones, actividades y operaciones, el registro de resultados, estadísticas y otros instrumentos de registro formal de los alcances obtenidos, la interpretación de los acuerdos, memorandos, normas, políticas y todos los aspectos formales que se asientan por escrito para el cumplimiento de las funciones y actividades en la administración cotidiana de las empresas.

Como es fácil observar, esta técnica tiene muchos alcances, y para muchos profesionales de auditoría es la forma más importante de evaluar a las empresas; además, no sólo sirve para aplicaciones en una auditoría tradicional, sino también como un importante apoyo en los diferentes tipos de auditoría de sistemas computacionales; claro está, adaptándola a las características específicas de evaluación de los sistemas computacionales.

A continuación, se presentan algunos ejemplos de la aplicación de esta técnica en la auditoría de sistemas computacionales:

• Evaluar el desarrollo de las operaciones y funcionamiento del sistema, mediante la revisión y el seguimiento de las instrucciones plasmadas en los manuales e instructivos de operación, manuales de usuarios, manuales del sistema y, en sí, de los flujogramas de actividades, procedimientos y de otros documentos que especifican la manera de operar los sistemas computacionales.

• Evaluar la existencia y cumplimiento de las normas, políticas, lineamientos y reglamentos de uso del área de sistemas y otros documentos que regulan los derechos y obligaciones del personal y los usuarios del sistema, a fin de valorar el desarrollo correcto de sus funciones y actividades, así como el uso adecuado de los sistemas computacionales.

• Revisar el uso y registro adecuados de documentos (bitácoras) para el control del software, hardware, la información de las bases de datos, el acceso del personal, de los

usuarios y de todas las personas que tienen acceso al centro de cómputo, así como las funciones y actividades plasmadas en los documentos del área utilizados para la administración y control de los sistemas computacionales.

4.5 Matriz de Evaluación

La matriz de evaluación es uno de los documentos de recopilación más versátiles y de mayor utilidad para el auditor, debido a que por medio de este documento es posible recopilar una gran cantidad de información relacionada con la actividad, operación o función que se realiza, así como apreciar anticipadamente el cumplimiento de dichas actividades.

Esta herramienta consiste en una matriz de seis columnas, de las cuales la primera corresponde a la descripción del aspecto que será evaluado y las otras cinco a un criterio de calificación descendente (o ascendente), en las que se anotan los criterios de evaluación para acceder a esa calificación.

Esta matriz de evaluación es un documento muy útil para el auditor de sistemas, debido a que le permite realizar cualquier tipo de valoración acerca del cumplimiento de una función específica de la administración del centro de cómputo, ya sea en la verificación de una serie de actividades de cualquier función del área de sistemas, del sistema computacional, del desarrollo de proyectos informáticos, del servicio a los usuarios del sistema o de muchas otras actividades exclusivas del área de sistemas de la empresa; además tiene la gran ventaja de poder valorar dicho cumplimiento con varios criterios que van desde lo excelente hasta lo pésimo.

A continuación, se verán los siguientes puntos para la elaboración de parámetros de evaluación de matriz:

• **Excelente.** Es cuando se califica con un 10, el 100% o la cifra considerada como el máximo posible que se pueda alcanzar. Esta calificación se utiliza cuando el desarrollo del trabajo, el cumplimiento de las funciones, el servicio o cualquier otro aspecto se cumplen con la mayor calidad y excelencia posibles.

• **Bueno.** En este punto se califica con un 9, el 90% o la cifra considerada como la siguiente en la escala. Esta calificación se utiliza cuando el desarrollo del trabajo es

altamente satisfactorio, pero existen algunos aspectos menores que impiden su total cumplimiento, ya sea de funciones, al otorgar el servicio o en cualquier otro aspecto.

• **Suficiente.** En este punto se califica con un 8, el 80% o la cifra considerada como la escala normal o la equivalente a ésta. Esta calificación se utiliza cuando el cumplimiento en el desarrollo del trabajo es satisfactorio, pero se considera como el mínimo necesario para ejecutar lo encomendado. Aquí se admiten algunos aspectos menores que impiden el cumplimiento total, ya sea de funciones, al otorgar el servicio o en cualquier otro aspecto de la actividad normal.

• **Regular.** En este punto se califica con un 7, el 70% o la cifra considerada como la mínima aceptable. Esta calificación se utiliza cuando el desarrollo del trabajo es francamente deficiente. Es decir, cuando el desarrollo del trabajo no es nada satisfactorio, pero se evalúa como el mínimo necesario para realizar la tarea encomendada. Aquí se cumple parcialmente con el trabajo, pero dentro de un rango muy por debajo de lo normal; apenas lo suficiente para efectuar lo encomendado, ya sean funciones, otorgamiento del servicio o cualquier otro aspecto.

• **Deficiente.** En este punto se califica con un 6, el 60% o la cifra considerada como la escala menor de lo aceptable. Esta calificación se utiliza cuando el desarrollo del trabajo es francamente deficiente y queda dentro de un rango muy por debajo de lo mínimo aceptable para realizar la tarea encomendada. Aquí se califican todos aquellos aspectos de incumplimiento que no satisfacen en lo más mínimo lo evaluado.

Es conveniente señalar que para diseñar correctamente este tipo de matriz se debe determinar, lo más detallada y claramente posible, el contenido de cada uno de los aspectos que serán evaluados, así como su calificación, a fin de que no exista ninguna posibilidad de desviación; estas calificaciones se establecen en una escala que va desde el máximo rango posible (excelente) hasta el mínimo rango (deficiente o insuficiente).

4.6 Listas de verificación

Éste es uno de los métodos de recopilación y evaluación de auditoría más sencillos, más cómodos y más fáciles de utilizar, debido a la simplicidad de su elaboración, la comodidad en su aplicación y por la facilidad para encontrar desviaciones, lo cual la hace una de las herramientas más confiables y utilizables para cualquier revisión.

Esta herramienta consiste en la elaboración de una lista ordenada, en la cual se anotan todos los aspectos que se tienen que revisar del funcionamiento, de sus componentes, del desarrollo de una actividad, del cumplimiento de una operación o de cualquier otro aspecto relacionado con la evaluación de un área; esta lista se complementa con una o varias columnas en las que se califica el cumplimiento del aspecto evaluado. Por lo general se describe el cumplimiento, se tacha el incumplimiento (X) o se deja en blanco. Con esto se identifica a simple vista el cumplimiento o incumplimiento del aspecto evaluado.

4.7 Entrevistas

Estas obtienen información sobre lo que se auditará; además, bien aplicada, les permite obtener guías que serán importantes para su trabajo, e incluso, muchas veces se entera de tips que le permitirán conocer más sobre los puntos que puede evaluar o debe analizar y mucha más información.

La entrevista podría entenderse como la recopilación de información que se realiza en forma directa, cara a cara y a través de algún medio de captura de datos, es decir, el auditor interroga, investiga y confirma directamente con el entrevistado sobre los aspectos que está auditando; en la aplicación de esta técnica, el auditor utiliza una guía de entrevista, la cual contiene una serie de preguntas preconcebidas que va adaptando conforme recibe la información del entrevistado, de acuerdo con las circunstancias que se le presentan y en busca de obtener más información útil para su trabajo.

Ciclo de la entrevista de auditoría:

Es conveniente señalar que para realizar una entrevista adecuada es indispensable entender y seguir un procedimiento bien estructurado, cuya eficacia en las auditorías tradicionales y en las ciencias sociales, donde es muy utilizada esta técnica, está plenamente comprobada. Esto le servirá al auditor llevar a cabo una buena investigación, apoyado en una serie de preguntas previamente establecidas y enfocadas al objetivo de la entrevista; con este método se busca captar una mayor información sobre lo que se auditará; además, esta información es más valiosa que la que se puede obtener por medio de un cuestionario, una observación o cualquier otra técnica de auditoría.

El siguiente procedimiento es indispensable para realizar una buena entrevista:

Inicio

Apertura

Cima o clímax

Cierre

4.8 Cuestionarios

Los cuestionarios son la recopilación de datos mediante preguntas impresas en hojas o fichas, en las que el encuestado responde de acuerdo con su criterio; de esta manera, el auditor obtiene información útil que puede concentrar, clasificar e interpretar por medio de su tabulación y análisis, para evaluar lo que está auditando y emitir una opinión sobre el aspecto investigado.

El cuestionario tiene la gran ventaja de que puede recopilar una gran cantidad de información, debido a que contiene preguntas sencillas cuyas respuestas no implican ninguna dificultad; además, como en otros métodos, su aplicación es de carácter impersonal y libre de influencias y compromisos para el entrevistado.

Ventajas y desventajas de los cuestionarios:

Los cuestionarios son los instrumentos más populares para la recopilación de información, sobre todo para la información relacionada con las auditorías de cualquier tipo. Por esta razón son muy utilizados y tienen muchas ventajas para obtener grandes volúmenes de datos, aunque también tienen grandes desventajas que limitan su aplicación.

Ventajas

• Facilitan la recopilación de información y no se necesitan muchas explicaciones ni una gran preparación para aplicarlos.

• Permiten la rápida tabulación e interpretación de los datos, proporcionándoles la confiabilidad requerida.

• Evitan la dispersión de la información requerida, al concentrarse en preguntas de elección forzosa.

• Por su diseño, los cuestionarios son muy rápidos de aplicar y ayudan a captar mucha información en poco tiempo.

• En el ambiente de sistemas es fácil capturar, concentrar y obtener información útil a partir de las respuestas, mediante el uso de la computadora. Incluso se pueden proyectar los datos y hacer gráficas.

• Hacen impersonal la aportación de respuestas; por lo tanto, en una auditoría ayudan a obtener información útil y confiable, si se plantean bien las preguntas.

Desventajas

• Falta de profundidad en las respuestas y no se puede ir más allá del cuestionario.

• Se necesita una buena elección del universo y de las muestras utilizadas.

• Pueden provocar la obtención de datos equivocados si se formulan deficientemente las preguntas, si se distorsionan o si se utilizan términos ilegibles, poco usados o estereotipados.

• La interpretación y el análisis de los datos pueden ser muy simples si el cuestionario no está bien estructurado o no contempla todos los puntos requeridos.

• Limitan la participación del auditado, ya que éste puede evadir preguntas importantes o se puede escudar en el anonimato que dan los cuestionarios.

• Hacen impersonal la participación del personal auditado, por lo que la aportación de la información útil para la auditoría es limitada.

• Denotan la falta de experiencia y pocos conocimientos del auditor que las aplica, si éste no plantea ni estructura correctamente las preguntas, lo cual puede provocar que su trabajo sea rechazado.

Método para diseñar y aplicar los cuestionarios:

Para aplicar correctamente un cuestionario se necesita un procedimiento específico que permita utilizar eficientemente este tipo de instrumentos de auditoría; basándonos en ello, a continuación, se presenta los siguientes pasos:

- Determinar el objetivo del cuestionario
- Elaborar un borrador del cuestionario
- Aplicar una prueba piloto
- Elaborar el cuestionario final
- Determinar el universo y la muestra
- Aplicar el cuestionario
- Tabular la información del cuestionario y elaborar gráficas y cuadros

- Interpretar los resultados
- Elaborar las observaciones

CASO PRÁCTICO

1. Basándose en los siguientes datos, elija un método o técnica para evaluar los sistemas y la red informática de la empresa. Realice un Informe.

La empresa Dulces Nacionales Mexicanos tiene presencia en el occidente del país y cuenta con un corporativo en Guadalajara, una planta de producción en Lagos de Moreno y otra en Cd. Guzmán. Cuentan con un sistema telefónico basado en PBX. En el corporativo tienen una red con 27computadoras la cual presenta frecuentes interrupciones, tienen 6 impresoras, 4 láser y 2 de matriz de puntos con un número alto de impresión personal y no institucional. El cableado no es estructurado y basan su funcionamiento en 3 Switches de 24 puertos interconectados entre sí, no existen políticas definidas en cuanto al empleo de la red y equipo de cómputo, por lo que los usuarios instalan programas de todo tipo sin control. Cuenta con acceso a Internet por un enlace privado (DS0) el cual representa una renta mensual de $1,500.00. La productividad entre los ejecutivos no es muy alta y no hay restricciones de acceso a Internet. El mes pasado tuvieron una infección masiva de computadoras por un virus, lo que ocasiono 2 días sin uso del equipo de cómputo, lo que represento un pico en el trabajo regular del equipo de sistemas, el cual está solicitando aumentar su plantilla de 5personas (1 gerente, 1 administrador de la red y 3 operadores, a 2 personas más). El departamento producción requiere un servidor para instalar un programa de planeación de la producción que recientemente se lo ha presentado. RRHH y Administración requieren comunicarse con los departamentos homónimos en las plantas de manera frecuente y segura para la transmisión y uso de archivos confidenciales debido a un proyecto de reestructuración y adopción de la norma ISO/9000 en administración y producción. La facturación mensual del corporativo asciende en promedio a $55,0000.00 y la tendencia es a aumentar. Paradójicamente, los clientes han empezado a quejarse de que cada vez es más difícil

comunicarse a ventas para la puesta de pedidos. En las plantas tienen redes con 17 y 24 computadoras respectivamente. Tienen un departamento de sistemas, el cual no se da abasto resolviendo la problemática de la operación diaria. Se conectan a Internet por línea telefónica y el cableado es muy inestable y lento. El Gerente de sistemas, que no tiene formación en informática, sino en contabilidad, solicita asesoría profesional para proponer un proyecto informático que les ayude a resolver la problemática, aumentarla productividad, reducir los gastos de operación y mejorar la comunicación tanto entre las plantas como con sus clientes. No cuentan con mucho dinero, pero están abiertos a propuestas.

BIBLIOGRAFÍA:

- MUÑOZ RAZO, Carlos. (2002). AUDITORÍA EN SISTEMAS COMPUTACIONALES. Prentice Hall.
- Sandoval, Hugo. (2012). INTRODUCCIÓN A LA AUDITORÍA. Primera edición. ISBN 978-607-733-137-7. Red Tercer Milenio S.C. México. Recuperado en: http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf.
- Heredero C, López J, Romo S, Medina S. (2011). Organización y Transformación de los Sistemas de Información en la Empresa. Esic Editorial. España.
- PINILLA, José D. Auditoría Informática un Enfoque operacional. Editorial Ecoe.

V. El Control y Riesgos en el uso de las Redes

OBJETIVOS:

- Identificar, analizar y evaluar, los riegos a los cuales se expone el servicio de interconexión de la red.
- Desarrollar e implementar planes de tratamiento para los riesgos.

¿DE QUÉ SE TRATA ESTA SECCIÓN DE APRENDIZAJE?

Se presenta una clasificación de los principales tipos de ataques contra las redes informáticas, así como cuáles podrían ser sus consecuencias para los sistemas víctimas de cada ataque.

Además de controles para minimizar o el eliminar los riesgos, a los cuales se expone el servicio de interconexión desarrollando e implementado las alternativas seleccionadas para la mitigación de la magnitud de los riesgos.

V. El Control y Riesgos en el uso de las Redes

5.1 Análisis de Riesgos en el uso de las Redes

5.1.1 Definición de Riesgo

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio (o conjunto de activos) o en toda la organización. Este impacto se puede producir debido a que una amenaza explote vulnerabilidades para causar pérdidas o daños.

El riesgo se caracteriza por una combinación de dos factores. La probabilidad de que ocurra el incidente no deseado y su impacto.

Cualquier modificación en activos, amenazas, vulnerabilidades y salvaguardad puede tener efectos significativos en el riesgo. La rápida detección o el conocimiento de cambios en el entorno o en el sistema facilitan la toma de decisiones adecuadas.

5.1.2 Análisis del Riesgo

El análisis de riesgos debe identificar los riesgos a su red, los recursos de red, y los datos. Esto no significa que debe identificar cada punto de entrada posible a la red, ni los medios posibles del ataque. El intento de un análisis de riesgo es identificar las partes de su red, asignar una calificación de amenaza para cada parte, y aplicar un nivel adecuado de seguridad. Esto ayuda a mantener un equilibrio factible entre la seguridad y el acceso de la red necesario.

Asignar a cada recurso de red uno de los siguientes tres niveles de riesgo:

- **Sistemas de bajo riesgo** o datos que, de verse comprometidos (datos observados por el personal no autorizado, datos corruptos, o datos perdidos) no se interrumpiría el negocio ni causaría ramificaciones económicas y legales. El sistema objetivo o los datos se puede recuperar fácilmente y no permite el acceso adicional de otros sistemas.
- **Los sistemas de riesgo mediano** o los datos que sí estuvo comprometido (los datos vistos por el personal no autorizado, los datos corrompidos, o los datos perdido) causaría una interrupción leve en el negocio, legal de menor importancia o las ramificaciones económicas, o proporcionan el acceso adicional a otros

sistemas. El sistema objetivo o los datos requieren un esfuerzo leve para restaurarse o el proceso de restauración es perturbador para el sistema.

- **Sistemas de Alto Riesgo** o datos que, e verse comprometidos (datos observados por el personal no autorizado, datos corruptos, o datos perdidos) causarían una interrupción extrema en el negocio, causarían ramificaciones económicas o legales importantes, o amenazarían la integridad o la seguridad de una persona. El sistema objetivo o los datos requieren mucho esfuerzo para restaurarse o el proceso de restauración es perturbador al negocio u otros sistemas.

Asignar un nivel de riesgo a cada uno de los siguientes:

- dispositivos de núcleo de la red,
- dispositivos de distribución de redes
- , dispositivos de acceso a redes,
- dispositivos de supervisión de redes (monitores SNMP y sondeos RMON),
- dispositivos de seguridad de la red (RADIUS y TACACS),
- sistemas del correo electrónico,
- servidores de archivo de red,
- servidores de impresión de redes,
- servidores de aplicación de redes (DN y DHCP),
- servidores de aplicación de datos (Oracle u otras aplicaciones autónomas),
- equipos de escritorio,
- y otros dispositivos (servidores de impresión y equipos de fax independientes de la red).

Los equipos de red tal como switches, routers, servidores DNS, y servidores DHCP permiten acceso adicional a la red y, por lo tanto, son dispositivos de riesgo moderado o alto. También es posible que la corrupción de este equipo cause el colapso de la red. Dicha falla puede ser extremadamente perjudicial para el negocio.

Una vez asignado un nivel de riesgo, es necesario identificar los tipos de usuarios de ese sistema.

La identificación del nivel de riesgo y del tipo de acceso necesarios de cada sistema de red forma la base de la matriz de seguridad. La matriz de seguridad proporciona una referencia rápida para cada sistema y un punto de partida para otras medidas de seguridad, tales como crear una estrategia adecuada para restringir el acceso a los recursos de red.

5.1.2.1 Tipos de Ataques

Un ataque a las redes de datos, consiste en aprovechar una vulnerabilidad de un sistema informático (sistema operativo, programa de software o sistema del usuario) con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Entre los tipos de ataques se pueden mencionar

5.1.2.2 Troyanos

Troyanos (Trojans): (a veces llamado Caballo de troya). Es un pequeño programa generalmente alojado dentro de otra aplicación (un archivo) normal. Su objetivo es pasar inadvertido al usuario e instalarse en el sistema cuando este ejecuta el archivo “huésped”, así queda activo en el sistema y abre un puerto de entrada a esa computadora. De esta manera la PC queda expuesta y puede ser accedida remotamente. Permitiendo a una persona acceder a la computadora infectada o recolectar datos y enviarlos por Internet a un desconocido. Luego de instalarse, pueden realizar las más diversas tareas, ocultas al usuario. En la teoría, un troyano no es virus, ya que no cumple con todas las características de estos, pero debido a que estas amenazas pueden propagarse de igual manera, suele incluírselos dentro del mismo grupo. Actualmente se los utiliza para la instalación de otros malware como backdoors y permitir el acceso al sistema al creador de la amenaza. Algunos troyanos, simulan realizar una función útil al usuario a la vez que también realizan la acción dañina. La similitud con el “caballo de Troya” de los griegos es evidente y debido a esa característica recibieron su nombre.

5.1.2.3 Anonimato

El anonimato en las redes se caracteriza por la capacidad de realizar cualquier acceso, comunicación o publicación en la red sin que terceros tengan la posibilidad de identificar o localizar al autor de dicha acción.

La privacidad en la navegación es un principio de internet. Por un lado, preserva la libertad de los ciudadanos y permite el libre crecimiento personal, cultural y político, sobre todo en aquellos países en los que existen regímenes represivos.

Por otro lado, el anonimato supone una ventaja para la realización de actividades delictivas en las redes (violación de la propiedad intelectual, spam, ciberacoso, injurias, estafa, robo de identidad, pederastia, etc.), y sobre todo para el encubrimiento de actividades o agresiones en el caso de conflictos asimétricos o terrorismo. Esto último incluye desde los filtrados de información, actividades de inteligencia en fuentes abiertas, acciones de propaganda, mando y control, hacking y ciberguerra, etc. Es más, sin que fuese posible sortear la identificación, muchas de estas últimas acciones no serían viables.

Las variables que definen el anonimato son: “quién soy”, “dónde estoy” y “qué hago”. Estas tres variables son distintas, pero íntimamente relacionadas entre sí, de forma que en muchos casos es posible deducir una de otra. Por ejemplo, si no se sabe quién soy o dónde estoy, mi comportamiento en la red no se me puede atribuir con facilidad, por el contrario, si se conoce dónde estoy y qué estoy haciendo, se puede inferir quién soy. En particular, “quién soy” es una variable mediatizada por la asimilación ordenador-usuario ya que siempre se accede a través de un terminal. Esta identidad es cada día más estrecha, pues los dispositivos son cada vez más personales, aunque existen recursos para identificarnos por encima del sistema que estemos utilizando para acceder a la red.

Para proteger estas tres variables existen dos tipos de salvaguardas: las legales y las técnicas. Las legales se derivan de los derechos fundamentales definidos en la Constitución y desarrollados en las leyes: el derecho al honor, la intimidad, la privacidad y el secreto de las comunicaciones.

Entre las técnicas se encuentran los mecanismos para ocultar la identidad, la localización y los servicios accedidos.

5.1.2.4 Spyware y web-bug

Spyware es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador. El término spyware también se utiliza más ampliamente para referirse a otros productos que no son estrictamente spyware. Estos productos, realizan diferentes funciones, como mostrar anuncios no solicitados (pop-up), recopilar información privada, redirigir solicitudes de páginas e instalar marcadores de teléfono. Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha el ordenador (utilizando CPU y memoria RAM, reduciendo la estabilidad del ordenador), y funciona todo el tiempo, controlando el uso que se hace de Internet y mostrando anuncios relacionados. Sin embargo, a diferencia de los virus, no se intenta replicar en otros ordenadores, por lo que funciona como un parásito. La mayoría de los programas spyware son instalados como troyanos junto a software deseable bajado de Internet. Otros programas spyware recogen la información mediante cookies de terceros o barra de herramientas instaladas en navegadores web. Los autores de spyware que intentan actuar de manera legal se presentan abiertamente como empresas de publicidad e incluyen unos términos de uso, en los que se explica de manera imprecisa el comportamiento del spyware, que los usuarios aceptan sin leer o sin entender. Las consecuencias de una infección de spyware moderada o severa (aparte de las cuestiones de privacidad) generalmente incluyen una pérdida considerable del rendimiento del sistema (hasta un 50 % en casos extremos), y problemas de estabilidad graves (el ordenador se queda "colgado"). También causan dificultad a la hora de conectar a Internet.

Los **web bugs** son imágenes o gráficos que se insertan en el código fuente de una página web o dentro de un correo electrónico con un tamaño reducido e inapreciable al ojo humano (generalmente de 1 píxel de ancho por uno de alto).

Al igual que ocurre con las cookies, los web bugs se utilizan para captar información acerca de nuestra forma de navegar (la dirección IP de nuestro ordenador, el tipo y versión de navegador que se utiliza, sistema operativo, idioma, etc.).

5.1.2.5 Espías en Programas

Son aplicaciones que se autoinstalan en programas de un ordenador sin el consentimiento del usuario y que se ocupa de entrar en la información del equipo y rastrear la actividad habida en él, para después ser manipulada por terceros con el fin de ofrecer, por ejemplo, contenido comercial relacionado con aquello que ha realizado o buscado el usuario, o incluso de robar datos personales (como las claves de la cuenta bancaria), entre otras acciones que pueden alterar el funcionamiento de la red.

5.1.2.6 Net Bios, otros

NETBIOS. Recursos compartidos en red no protegidos. El protocolo SMB (Server Message Block), también conocido como CIFS (Common Internet File System), permite habilitar la compartición de recursos a través de la red. Muchos usuarios permiten el acceso a sus discos con la intención de facilitar el trabajo en grupo con sus colaboradores. Sin saberlo, están abriendo sus sistemas a cualquier atacante al permitir el acceso, tanto de lectura como de escritura, a otros usuarios de la red. Habilitar la propiedad de compartir archivos en máquinas Windows las hace vulnerables tanto al robo de información como a ciertos tipos de virus que se propagan con rapidez. Las máquinas Macintosh y UNIX son también vulnerables a ataques de este tipo si los usuarios habilitan la compartición de archivos.

Otros Ataques:

Otro ataque que puede darse son los **Ataques de denegación de servicio (DoS):**

Un ataque DoS colapsa totalmente un servidor y hace imposible (o muy lenta) la navegación a través de él. No sólo se pueden atacar servidores web, también servidores de correo electrónico, servidores DNS etc.

Un ataque DoS se puede “atenuar” mediante reglas específicas en el cortafuegos. Cuando desde una misma IP se realizan miles de peticiones, un servidor puede denegar el acceso a la IP atacante y de esa manera parar el ataque. El problema lo tenemos cuando el ataque es distribuido, porque el servidor no da abasto para bloquear todas las IP’s, y cada vez hay más y más y el servidor termina por saturarse.

Podemos clasificar los ataques de denegación de servicio en tres categorías:

- **Inundación de conexiones:** normalmente el protocolo que se usa es TCP, al ser conectivo, fiable y orientado a conexión. El propio protocolo TCP pide el reenvío de los paquetes perdidos y se encarga de la fragmentación y el re-ensamblado (no como UDP sobre IP). El atacante establece cientos de conexiones en el servidor hasta que que se colapsa y no puede aceptar las conexiones de usuarios legítimos.
- **Inundación de ancho de banda:** el usuario malintencionado envía muchos paquetes al servidor, impidiendo que los paquetes legítimos puedan llegar a él, no hay suficiente ancho de banda para más paquetes.
- **Ataque de vulnerabilidad:** si en el servidor hay alguna vulnerabilidad, el atacante se centra en explotarla mandando mensajes construidos específicamente para provocar el fallo de la máquina.

Para colapsar un servidor por inundación de ancho de banda, el ataque ha de ser distribuido (DDoS) ya que actualmente los servidores tienen un gran ancho de banda. Además, sería muy fácil detectarlo ya que sólo sería desde una IP (en DoS no distribuido). El ancho de banda del ataque se debe acercar al ancho de banda máximo de dicho servidor para colapsarlo.

El problema de los ataques distribuidos es que no sabes si el que realiza las peticiones es un atacante, o el legítimo usuario, por tanto, es mucho más difícil de detectar y, sobre todo, mucho más difícil defenderse de ellos.

5.1.3 Diseño de Estrategias para mitigar el Riesgo

5.1.3.1 Escaneo estado de puertos

El mapeo de puertos se basa en identificar los puertos abiertos con el fin de analizarlos internamente en uno o varios hosts que integran una red. El escaneo de puertos es utilizado para optimizar las funciones de seguridad y utilidad de las redes, de igual forma se logra transformar en una acción peligrosa que se usa para averiguar zonas críticas sensibles y violentar el ingreso al sistema de información.

Los sistemas informáticos pueden presentar puertos abiertos que son omitidos por los profesionales de seguridad, ocasionado que los puertos no sean supervisados y la información circule por medio de estos desprovistos de controles de seguridad,

produciendo una vulnerabilidad del sistema de información, Lo anterior es producto de errores en la configuración de los procedimientos de seguridad, en los cortafuegos por defecto se dejan diversos puertos abiertos, y los encargados de la administración de los cortafuegos omiten analizar cuidadosamente la configuración para identificar todos los puertos utilizables .

Cuando los puertos TCP/IP (interfaces de transmisión no físicas para conmutación de datos y servicios en una red) se encuentran abiertos son atractivos para los atacantes los cuales pueden ejecutar pruebas de intrusión y vulnerar la seguridad de una red. Una técnica usual para revelar los puertos abiertos es el sondeo con el objetivo de evaluar los servicios aprovechables en una red, para identificar puertos vulnerables se remite una sucesión de paquetes deficientes a una dirección IP inexistente en la red, estos son filtrados por el firewall el cual los obstruye y no accede a enrutarlos, cuando no se efectúa el filtrado faculta el paso de los paquetes los cuales no es factible enrutarlos y al no poder enrutarlo apropiadamente, el firewall envía avisos de error ICMP (Protocolo de Mensajes de Control de Internet: accede gestionar y notificar errores de los hosts de una red más no permite su modificación) mostrando que los paquetes no se filtraron.

5.1.3.2 Test

Existen dos tipos de test: Test de penetración y test de seguridad.

Un test de penetración (también denominado hacking ético y white-hat-hacking o red-teaming) es un conjunto de métodos que permiten valorar el estado o actitud de seguridad de un sistema de red utilizando para ello una simulación no destructiva de diversos ataques. Se trata de un intento legal de acceder a la red de la empresa para encontrar sus eslabones más débiles, el que hace el test sólo reporta lo encontrado.

Un test de seguridad es más que un intento de acceder, también incluye el análisis de la política y procedimientos de seguridad de la compañía, las personas que realizan el test ofrecen soluciones para proteger la red evaluada.

Existen diversas razones para realizar un test de penetración:

- Determinar los fallos-defectos y vulnerabilidades de una empresa.
- Proporcionar una métrica cuantitativa para poder evaluar sistemas y redes.
- Medir contra líneas de fondo pre-establecidas.

- Determinar riesgos para la organización.
- Designar controles para mitigar los riesgos identificados.

En un test de penetración se pueden identificar las siguientes fases:

1. Fase de preparación.

En esta fase se Identifican los objetivos: sitios Web de la compañía, servidores de correo, extranets, etc. Se firma el contrato y se establece un acuerdo de protección contra cualquier cuestión legal. Los contratos especifican claramente los límites y peligros del test. Especificar los test DoS de ingeniería social, etc. Se debe especificar la ventana temporal de los ataques, el tiempo total del test. Se debe indicar el nivel de conocimiento previo de los sistemas y las personas claves a las que se les hace consciente del test.

2. Fase de footprinting.

En esta fase es crucial recoger el máximo de información sobre el objetivo: servidores DNS, rangos de IP, contactos administrativos y problemas revelados por los administradores.

3. Fase de descubrimiento, enumeración y fingerprinting.

Esta fase se trata de:

- Determinar los objetivos específicos.
- Identificar servicios y puertos UDP/TCP abiertos.
- Enumerar sistemas operativos utilizados.
- Respuestas a comandos de protocolos varios (TCP y ICMP).
- Escaneo de puertos/servicios: conexiones TCP, TCP SYN, TCP FIN, etc. Se utilizan herramientas como: Nmap, el objetivo es recoger y obtener información de la forma más sigilosa posible. También se revisa la información de red y se confirma lo que se sabe de las redes.

4. Fase de exploración e identificación de vulnerabilidades.

Son posibles vulnerabilidades:

- Configuración no segura.
- Contraseñas débiles.
- Vulnerabilidades sin parches en: servicios, sistemas operativos y aplicaciones.
- Vulnerabilidades posibles en servicios y sistemas operativos.
- Programación no segura.

- Control de acceso débil. Se utilizan herramientas de detección y sitios Web de información de vulnerabilidades. Para contraseñas débiles: contraseñas por defecto, ataque por fuerza bruta y diccionario, ingeniería social, escucha del tráfico no cifrado (pop3, telnet, ftp, etc.). Para programación no segura: inyección SQL, escucha del tráfico. Para el control de acceso débil: uso de lógica de la aplicación e inyección SQL.

Entre los objetivos de esta fase está el análisis de la configuración, se identifican y analizan los firewall/gateways.

5. Fase de valoración, ataque y explotación de vulnerabilidades.

El objetivo es obtener la máxima información del punto que se va a poner a prueba, ganar acceso normal, el escalado de privilegios, así mismo obtener acceso a otros sistemas conectados y utilizar DoS.

Se realizan:

- Ataques a la infraestructura de red: conectarse a la red a través de módem, identificar debilidades en TCP/IP, NetBIOS, realizar inundación de la red para causar DoS.
- Ataques a los sistemas operativos: ataque a los sistemas de autenticación, explotación de las implementaciones de los protocolos, explotación de las configuraciones no seguras, rotura de la seguridad del sistema de ficheros.
- Ataques a aplicaciones específicas: explotar implementaciones de protocolos de aplicación smtp, http, ganar acceso a las BDs de aplicación, inyecciones SQL, spamming (correo basura).

En esta fase se comprueba la seguridad de los dispositivos. Para ello se aumenta el network mapping, se escanean los dispositivos en busca de vulnerabilidades y se explotan vulnerabilidades de seguridad que estén solas.

6. Fase de análisis de intrusiones y riesgos/impactos.

El objetivo es realizar un análisis de escenario de la red y explotar las posibles exposiciones de la red.

7. Fase de reporting.

El objetivo es informar de todo lo obtenido y proponer soluciones de seguridad prácticas.

En un entorno TIC el modelo de test de penetración de seguridad consta de cuatro niveles, que de fuera hacia dentro son:

Nivel 1: ataques externos (usuario no informado).

Nivel 2: Ataques externos (usuario con conocimiento).

Nivel 3: Ataques internos.

Nivel 4: Ataques a las aplicaciones/bases de datos.

Se pueden identificar tres metodologías de test de penetración:

1. Modelo white-box. El que hace el test se le dice todo acerca de la topología y tecnología de la red, está autorizado para entrevistar al personal de TIC y a los empleados de la compañía, esto hace el trabajo un poco más fácil.

2. Modelo black-box. El personal de la compañía no sabe nada acerca del test. El que hace el test no conoce los detalles de la red, su trabajo incluye averiguarlos. Aquí se comprueba si el personal de seguridad puede detectar un ataque.

3. Modelo gray-box. Es un modelo híbrido de los dos modelos anteriores. La compañía proporciona al que hace el test cierta información parcial.

5.1.3.3 Privacidad

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos que están compuestos de elementos de transmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.) y servicios de apoyo (sistema de nombres de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicios de autenticación, etc.). Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (servidores, teléfonos, ordenadores personales, teléfonos móviles, etc.). Es por esto que la privacidad es un tema crucial que debemos tomar en cuenta, se presentan algunos requisitos para mantener la privacidad en las redes

Requisitos para Mantener la Privacidad de las Redes

Las redes deben cumplir los siguientes requisitos o características para mantener su privacidad y poder ser más seguras ante las posibilidades de intrusión.

1. Disponibilidad: significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta

característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones de la empresa.

2. Autenticación: confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos, la autenticación de los sitios web, etc.

3. Integridad: confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica.

4. Confidencialidad: protección de las comunicaciones o los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación. Es preciso tener en cuenta todos los factores que pueden amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

5.1.3.4 Pruebas de Seguridad, otros

En las pruebas se efectúa una relación de servicios activos de acuerdo con su utilidad y la confiabilidad de los datos almacenados. A través del empleo de herramientas de pentesting se identifica componentes activos que se encuentran en la red, mediante una dirección IP para localizar las vulnerabilidades existentes en el software y hardware y prevenir percances de seguridad.

Otros:

Seguridad ante programas malignos:

Se establecerán las medidas y procedimientos que se requieran para la protección contra virus y otros programas dañinos que puedan afectar los sistemas en explotación, así como para evitar su generalización, especificando los programas antivirus utilizados y su régimen de instalación y actualización.

La protección contra códigos maliciosos se basará en el empleo de medidas de prevención, detección y recuperación, en la necesidad de la seguridad, y en controles apropiados de acceso al sistema. Las siguientes pautas serán consideradas:

- Establecimiento de políticas que instituyan la prohibición del uso de software no autorizado y la protección contra los riesgos asociados a la obtención de archivos y software por redes externas o cualquier otro medio, indicando las medidas protectoras a adoptar.
- Revisiones regulares del contenido de datos y software que soportan los procesos de gestión de la entidad y de la presencia de archivos no aprobados o modificaciones no autorizadas.
- La instalación y actualización regular de programas antivirus que exploren las computadoras y los soportes de forma rutinaria o como un control preventivo para la detección y eliminación de código maliciosos, las verificaciones incluirán:

  a) Comprobación de archivos en medios electrónicos u ópticos, y archivos recibidos a través de la red, para verificar la existencia de código malicioso, antes de su uso.

  b) Comprobación de todo archivo adjunto a un correo electrónico o de cualquier descarga antes de su uso. Realizar esta comprobación en distintos lugares, por ejemplo, en los servidores de correo, en las computadoras terminales o a la entrada de la red de la organización.

  c) Comprobación de páginas web para saber si existe en ellas código malicioso.

- La definición de procedimientos y responsabilidades de gestión para la protección de los sistemas contra código malicioso, la capacitación, su uso, la información de los ataques de los virus y las acciones de recuperación.

- La implementación de medidas para la recuperación ante ataques de código malicioso, incluyendo los datos y software necesarios de respaldo y las disposiciones para la recuperación.
- La implementación de procedimientos para obtener información sobre nuevos códigos malicioso, incluyendo los datos y software necesarios de respaldo y las disposiciones para la recuperación.
- La implementación de procedimientos para verificar la información relativa al software malicioso y asegurarse que es real. Los encargados de esta actividad deben poder diferenciar los códigos maliciosos reales de los falsos avisos de código malicioso, usando fuentes calificadas. Se advertirá al personal sobre el problema de los falsos avisos de código malicioso y qué hacer en caso de recibirlos.

5.2 Evaluación de Control en Redes

5.2.1 Control en la Creación de la Red

Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de redes.

Objetivos:

- Garantizar que el hardware y software se adquieran siempre y cuando tengan la seguridad de que los sistemas redes proporcionaran mayores beneficios que cualquier otra alternativa.
- Garantizar la selección adecuada de equipos de redes.
- Asegurar la elaboración de un plan de actividades previo a la instalación.

Acciones que seguir:

- Elaboración de un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio.
- Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación.

- Elaborar un plan de instalación de equipo de redes y software (fechas, actividades, responsables) el mismo que debe contar con la aprobación de los proveedores del equipo.
- Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios de redes. Este proceso debe enmarcarse en normas y disposiciones legales.
- Efectuar las acciones necesarias para una mayor participación de proveedores.
- Asegurar el respaldo de mantenimiento y asistencia técnica.

5.2.1.1 Estación de Redes

Una red de datos bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de redes. Los dispositivos del sistema de redes podrían ser dañados si se manejan de forma inadecuada y eso se podría ocasionar pérdidas de dinero o información. Se debe analizar las disposiciones y reglas que ayuden a mantener su funcionamiento correctamente, además se debe tener en cuenta calendarios para realizar mantenimientos técnicos.

5.2.1.2 Servidores

Un servidor es una computadora que, formando parte de una red, provee servicios a otras computadoras denominadas clientes. Existe una gran variedad de servidores que desarrollan variadas funciones.

La Seguridad en los servidores es la protección de la infraestructura computacional y todo lo relacionado con esta incluyendo la información que esta contenga. Existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas, para minimizar los posibles riesgos a los medios o la información.

Cuando un sistema es usado como un servidor en una red pública, se convierte en un objetivo para ataques. Por esta razón, es de suma importancia para el administrador fortalecer el sistema y bloquear servicios.

Entre los controles que se pueden aplicar para mejorar la seguridad del servidor están:

- Mantenga todos los servicios actualizados para protegerse de las últimas amenazas.

- Utilice protocolos seguros siempre que sea posible.
- Proporcione sólo un tipo de servicio de red por máquina siempre que sea posible.
- Análisis periódicos de la seguridad de los servidores
- Supervise todos los servidores cuidadosamente por actividad sospechosa.
- Utilice sistemas de detección de intrusos en los servidores locales
- Normalización de hardware.
- Aplicación oportuna de parches de seguridad y correcciones de errores

5.2.1.3. Hardware de Comunicaciones

Abarcan todo el ambiente de la operación del equipo central de redes y dispositivo de comunicación, es necesario establecer controles para prevenir ataques o fallos en los sistemas.

Los controles tienen como fin:

- Prevenir o detectar errores accidentales que puedan ocurrir en el Centro de Redes durante un proceso.
- Evitar o detectar el manejo de equipo no autorizados por parte de los usuarios.
- Garantizar la integridad de los recursos informáticos.
- Asegurar la utilización adecuada de equipos acorde a planes y objetivos.

Controles:

- Diseño e implantación de un plan de contingencia como alternativa de comunicaciones para asegurar la continuidad de las comunicaciones.
- El acceso al centro de comunicaciones debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado.
- Implantar claves o password para garantizar operación de consola y equipo central (mainframe), a personal autorizado.
- Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y como responder ante esos eventos.
- Los operadores del equipo de hardware de comunicaciones deben estar entrenados para recuperar o restaurar información.

- Se deben implantar calendarios de mantenimiento técnico a los equipos de comunicaciones a fin de mantener un buen funcionamiento.
- Todas las actividades del hardware de comunicaciones deben normarse mediante manuales, instructivos, normas, reglamentos, etc.
- El proveedor de hardware deberá proporcionar lo siguiente:

Manual de operación de equipos

Manual de utilitarios disponibles

- Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras.
- Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, UPS, generadores de energía.
- Contar con hardware de comunicaciones de respaldo.
- Contratar pólizas de seguros para proteger los equipos.

5.2.2 Control en la Configuración de la Red

5.2.2.1 Físicos

El acceso físico a los ordenadores y equipos de red aumenta el riesgo de cualquier incidente. Debe configurarse la red para conceder acceso exclusivamente a quien lo necesite por sus funcione.

Las consecuencias de un ataque físico podrían llegar a ser graves, entre los infractores se pueden encontrar los propios usuarios o personas externas.

Es por esto por lo que al configurar la red se debe tener en cuenta la protección de los equipos de manera física.

Entre los controles físicos que se pueden establecer en la configuración de una red están:

- Diseño e implementación de políticas de seguridad de acceso físico, para que los equipos de comunicaciones estén en lugar cerrado y con acceso limitado.
- Aplicar normas y procedimientos para separar las actividades eléctricas del de cableado de red y de líneas telefónicas.
- Verificación de la utilización de equipos adecuados de monitorización de la red.
- Diseño e implementación de un plan de recuperación del sistema de comunicaciones.

5.2.2.2 Lógicos

Los ataques lógicos suelen ser muy frecuentes en las redes de datos, ya sea mediante algún tipo de virus o acceso no autorizado. Establecer controles en la configuración de la red ayudan a disminuir las vulnerabilidades y las amenazas a la red.

Entre los controles lógicos que se pueden establecer en la configuración de una red están:

- Autenticación de usuarios para conexiones externas.
- Identificación de los equipos en las redes
- Protección de los puertos de configuración y diagnóstico remoto.
- Separación en las Redes.
- Control de Conexiones a las Redes.
- Control del Enrutamiento en la Red
- Controles de acceso al sistema operativo.
- Separaciones de redes, por ejemplo, en bases a servicios de información, o grupos de usuarios o sistemas.
- Establecer mecanismos de autenticación y registro para las conexiones externas a la empresa o remotas.

5.2.3 Control en el Funcionamiento de la Red

Algunas medidas de control que se pueden poner en práctica en el funcionamiento de la red para evitar cualquier acceso o interrupción de actividad pueden ser las siguientes:

- Hay que asegurar que todos los datos sean procesados
- Garantizar la exactitud de los datos procesados
- Garantizar que se grabe un archivo para uso de la gerencia y con fines de auditoria
- Hay que asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.
- Utilizar un firewall, que no es más que un dispositivo localizado entre el ordenador anfitrión y una red, con el objeto de bloquear el tráfico no deseado de la red mientras permite el cruce de otro tráfico.
- Utilización y actualización de antivirus.

- Actualizar todos los sistemas, servidores y aplicaciones, ya que los intrusos por lo general a través de agujeros conocidos de seguridad.
- Desactivar los servicios innecesarios de redes.
- Realizar informes de seguimiento de monitorización de protocolos, estadísticas de errores en la transmisión.
- Eliminar todos los programas innecesarios.
- Analizar la red en busca de servicios comunes de acceso furtivo y utilizar sistemas de detección de intrusos los cuales permiten detectar ataques que pasan inadvertidos a un firewall y avisar antes o justo después de que se produzcan,
- Finalmente, establecer la práctica de crear respaldos o Backus. Hay muchos dispositivos de seguridad que pueden utilizar las empresas para contrarrestar las amenazas a las que están expuestas, por eso, con frecuencia muchas terminan utilizando soluciones como los firewalls, sistemas de detección de intrusos, redes virtuales, etc. para obtener la protección total que necesitan en materia de seguridad. Debido al incremento de las amenazas y la naturaleza dinámica de los ataques, es necesario adoptar prácticas eficientes e implementar políticas de seguridad que nos permitan manejar eficientemente este tipo de ataques.

5.2.4 Control de Personal

Las implicaciones del factor humano en la seguridad de las redes son elevadas. Todo el personal tanto interno como externo a la organización, debe conocer tanto las líneas generales de la política de seguridad corporativa como las implicaciones de su trabajo en el mantenimiento de la seguridad global.

Ya que existen diferentes relaciones con los sistemas de redes como pueden ser: operador, administrador, personal en general, directores, etc., así mismo se deben establecer controles para cada miembro del personal de la organización, de acuerdo con las funciones que realiza y su actividad como usuario de la red de datos.

5.2.4.1. Usuario del Sistema

Los controles de la red deben definir los derechos y las responsabilidades de los usuarios del sistema que utilizan los recursos de la red. A continuación, algunos ejemplos de controles aplicables a los usuarios de los servicios de red:

- Establecer lineamientos acerca del uso de los recursos de la red, tales como los usuarios restringidos.
- Enumerar actividades que se consideran como uso inadecuado de los recursos de la red.
- Reglas sobre la compartición de contraseñas, con otros usuarios de la red.
- Políticas de contraseñas para usuarios: con qué frecuencia deben cambiarla, y otros requerimientos.
- Orientar a los usuarios sobre responsabilidades o no de realizar respaldo de sus datos.
- Comunicar consecuencias para los usuarios que divulguen información que pueda estar restringida.
- Normativas para usos de correo electrónico e internet.

5.2.4.2. Perfiles de Usuarios

Entre los perfiles de usuario podemos encontrar los siguientes:

- Usuarios internos de los administradores responsables de los recursos de red.
- Usuarios internos privilegiados con necesidad de mayor acceso.
- Usuarios internos de usuarios con acceso general.
- Usuarios externos de socios con necesidad de acceder a algunos recursos.
- Otros usuarios externos o clientes.

Un correcto manejo de perfiles de usuarios es de gran ayuda para mitigar el riesgo en el uso de las redes, ya que a través de estos se crean niveles de acceso según las características de cada usuario.

5.2.4.3 Capacitación

Los ataques informáticos y los riesgos para las empresas se han vuelto más complejos, y eso se debe tener en cuenta en las estrategias y la gestión de seguridad para que sean efectivas.

No existe una empresa que esté totalmente libre del riesgo de sufrir un ataque de seguridad informática. Esta es una realidad. Sin embargo, conceptos como gestión, proactividad y educación, se vuelven cruciales al momento de implementar una estrategia de protección en las organizaciones, y para posteriormente mitigar de manera más eficaz los efectos y daños causados por los ataques.

Para mitigar la ocurrencia de ataques es importante la educación del usuario final. Es importante mantener a los usuarios alertas respecto de actividades sospechosas como, por ejemplo, solicitudes de contactos desconocidos o con perfiles poco convincentes en redes sociales, correos con súper ofertas, solicitudes de claves bancarias, etc. Para todo este tipo de eventos el usuario debe estar preparado en cómo responder de forma segura y sin poner en riesgo la información.

Todos los empleados deben recibir capacitación en materia de contraseñas, políticas de seguridad, etc. Esta capacitación puede abarcar los siguientes puntos:

- Garantizar que los empleados no anotan sus contraseñas por escrito (susceptibles de ser robadas).
- Garantizar que los empleados no revelan sus contraseñas en ningún tipo de comunicación a través de Internet, a menos que la comunicación esté cifrada.
- Animar a los empleados a crear contraseñas sólidas y usar una herramienta de gestión de contraseñas corporativas.
- Garantizar que los empleados no reutilizan sus contraseñas en distintas aplicaciones corporativas o en sus cuentas personales y corporativas.
- Los empleados utilizarán en algún momento la red informática de su empresa para visitar sitios web o registrarse para usar servicios tanto con fines personales como corporativos. Antes de enviar información, deben tratar de localizar el candado y el protocolo HTTPS en la barra de direcciones. Si el sitio web no está protegido, no deberán introducir ningún dato.

- Habilitar comunicaciones seguras a través de correo electrónico y ofrezca capacitación para mitigar los riesgos de sufrir ataques de phishing. Realice pruebas de simulación de ataques de phishing en la empresa para comprobar el grado de alerta de los empleados. Estas pruebas deben realizarse antes y después de la capacitación con el objetivo de medir los avances de los empleados.
- Asegurarse de estar preparado para responder de forma rápida y eficiente frente a un ciberataque. Transmitir este plan al resto de la organización en el programa de capacitación y designar a un encargado de garantizar que el plan se ejecuta. Anunciar a los empleados el plan de respuesta e informarles de los posibles tipos de incidentes y soluciones ayudará a recordar que ellos también son responsables de mantener la confidencialidad y minimizar el riesgo de fugas de información a fuentes externas.

CASOS DE ESTUDIO PRÁCTICO

1. Escáner de puertos: Nmap

El escaneo de puertos permite auditar máquinas y redes para saber qué puertos están abiertos. NMAP(Network Mapper) es una herramienta libre para la auditoría disponible para varias plataformas. Con esta herramienta se puede saber qué ordenadores están encendidos en la red, los puertos abiertos y qué servicio ofrecen, el sistema operativo que se está ejecutando en la máquina, si tiene firewall, etc.

Nmap usa un proceso de escaneado de tres pasos:

1) Nmap envía un ping a la máquina objetivo. El usuario puede elegir entre una solicitud de eco o de alguna técnica propia de nmap.

2) Se averigua el nombre del equipo a partir de su dirección IP.

3) Nmap escanea los puertos de la máquina utilizando la técnica seleccionada.

Se pueden utilizar unas quince técnicas distintas de sondeos de puertos: Tcp connect, TCP SYN, TCP FIN, ping, UDP scan, etc.

1. Instalar nmap en cualquier plataforma, y su interfaz gráfica Zenmap, o NMPFE, O knmap.

2. Ejecutar Znamp, introducir la dirección IP de la máquina a analizar, y seleccionar el tipo de escáner a realizar. ¿Qué puertos tiene abiertos la máquina estudiada? ¿Qué sistema operativo está corriendo?

3. Utiliza la consola para introducir las siguientes órdenes:

```
nmap -v -A www.google.es
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 P0 -p 80
```

4. Explica el significado de las órdenes introducidas en el punto 3, y del resultado obtenido.

5. Para escanear un determinado rango de puertos en una máquina:

nmap -p 1-80 direccion_IP

6. Para saber qué ordenadores de una red tienen un determinado puerto abierto se averigua de la siguiente manera:

nmap -p 139 192.168.1.0-255

Comprueba en tu red qué ordenadores tienen los puertos NetBios abiertos

7. Si queremos averiguar las versiones de los servicios se debe usar la opción -sV:
nmap -sV 192.168.1.1

8. Con la opción -O se puede averiguar qué sistema operativo tiene una máquina.
nmap -O 192.168.1.1

9.Nmap también dispone de una interfaz mediante página web denominada phpNmap. Instálala y compárala con la interfaz gráfica que hayas utilizado.

Ejercicio práctico 2:

1. Instala un software de gestión de contraseñas en tu equipo, explica cómo funciona y cuáles son sus ventajas.

BIBLIOGRAFÍA:

- Bartolín Javier. (2008). Seguridad en la Información, Ediciones PARAINFO. Madrid, España.
- Guindel Esmeralda. (2009). Calidad y seguridad de la Información y Auditoría Informática. Universidad Carlos III de Madrid. España.
- Alvarez Luis. (2005). Seguridad en Informática (Auditoría de Sistemas). Universidad Iberoamericana. México.
- Piattini, Mario G. del Peso, Emilio. (2001) Auditoría Informática un Enfoque Práctico. Editorial Computec.
- Xiomar Rojas D. Auditoría Informática. Editorial Universidad Estatal A Distancia. Costa Rica.
- LOTT, Richard W. Auditoría y Control del PED. Editorial Norma.
- ECHENIQUE, José A. Auditoría Informática. Editorial. Mc Graw-Hill.

VI. Auditoría de Red

OBJETIVOS:

- Conocer el proceso de planeación y ejecución de la auditoría de redes física y lógica.
- Desarrollar los controles y evaluar mediante la ejecución de la auditoría si estos son puestos en práctica.
- Conocer la planeación y ejecución de la auditoría en un entorno web.

¿DE QUÉ SE TRATA ESTA SECCIÓN DE APRENDIAJE?

Este capítulo abordará el enfoque principal de la asignatura que es la auditoría de redes, su proceso de planeación y establecimientos de controles y su respectiva ejecución evaluando la presencia o puesta en práctica de estos controles; ya que debido al persistente y continuo avance tecnológico en el ambiente de sistemas de redes, es preciso señalar que la práctica de la auditoría a los sistemas de redes de cómputo cada vez se vuelve más compleja, minuciosa y especializada; además, debido a los constantes cambios y avances en las redes computacionales obligan al auditor de sistemas a actualizarse constantemente, en especial en los sistemas de redes y también en los sistemas web, ya que es un área que va a un crecimiento acelerado.

VI. Auditoria de Red

6.1. Planeación y Ejecución de Auditoria de Redes.

Debido al persistente y continuo avance tecnológico en el ambiente de sistemas de redes, es preciso señalar que la práctica de la auditoría a los sistemas de redes de cómputo cada vez se vuelve más compleja, minuciosa y especializada; además, debido a los constantes cambios y avances en las redes computacionales obligan al auditor de sistemas a actualizarse constantemente, en especial en los sistemas de redes. Esto es necesario si el auditor quiere contar con el suficiente conocimiento informático que le permita analizar los principales rubros que conforman una red de cómputo.

El auditor es responsable en la auditoría de establecer los puntos que va a evaluar como lo considere necesario, de acuerdo con su experiencia, conocimientos y habilidades; siempre y cuando su objetivo sea obtener mejores resultados en su revisión. Todo de acuerdo con las características específicas de la red de cómputo que vaya a evaluar y con las peculiaridades de la administración de estos sistemas.

6.1.1. Planeación de Auditoria de Red Física.

Se establecen distintos riesgos para los datos que circulan dentro del edificio de aquellos que viajan por el exterior. Por tanto, ha de auditarse hasta qué punto las instalaciones físicas del edificio ofrecen garantías y han sido estudiadas las vulnerabilidades existentes.

En general muchas veces, se parte del supuesto de que si no existe acceso físico desde el exterior a la red interna de una empresa las comunicaciones internas quedan a salvo. Debe comprobarse que efectivamente los accesos físicos provenientes del exterior han sido debidamente registrados, para evitar estos accesos. Debe también comprobarse que desde el interior del edificio no se intercepta físicamente el cableado.

En caso de desastre, bien sea total o parcial, ha de poder comprobarse cuál es la parte del cableado que queda en condiciones de funcionar y qué operatividad puede soportar. Ya que el tendido de cables es una actividad irrealizable a muy corto plazo, los planes de recuperación de contingencia deben tener prevista la recuperación de comunicaciones.

Como objetivos de control se deben marcar la existencia de:

- Áreas controladas para los equipos de comunicación, previniendo así accesos inadecuados.
- Protección y tendido adecuado de cables y líneas de comunicación, para evitar accesos físicos.
- Controles de utilización de los equipos de pruebas de comunicación, usados para monitorizar la red y su tráfico, que impidan su utilización inadecuada.
- Atención específica a la recuperación de los sistemas de comunicación de datos en el plan de recuperación de desastres en sistemas de información.
- Controles específicos en caso de que se utilicen líneas telefónicas normales con acceso a la red de datos para prevenir accesos no autorizados al sistema o la red.

6.1.1.1. Ejecución de Auditoria de Red Física.

Lista de Control

Comprobar que:

F1. El equipo de comunicaciones se mantiene en habilitaciones cerradas con acceso limitado a personas autorizadas.

F.2. La seguridad física de los equipos de comunicación, tales como controladores de comunicaciones, dentro de las salas de computadoras sea adecuadas.

F.3 Sólo personas con responsabilidad y conocimientos están incluidas en la lista de personas permanentemente autorizadas para entra en las salas de equipos de comunicaciones.

F.4. Se toman medidas para separar las actividades de electricistas y personal de tendido y mantenimiento de tendido de líneas telefónicas, así como sus autorizaciones de acceso, de aquellas de personal bajo control de la gerencia ce comunicaciones.

F.5. En las zonas adyacentes a las salas de comunicaciones, todas las líneas de comunicaciones fuera de la vista.

F.6. Las líneas de comunicaciones en las salas de comunicaciones, armarios distribuidores y terminaciones de los despachos estarán etiquetadas con un código gestionado por la gerencia de comunicaciones, y no por su descripción física o métodos sin coherencia.

F.7 Existen procedimientos para la protección de cables y bocas de conexión que dificulten el que sean interceptados o conectados por personas no autorizadas.

F.8. Se revisa periódicamente la red de comunicaciones, buscando intercepciones activas o pasivas.

F.9. Los equipos de prueba de comunicaciones usados para resolver los problemas de comunicaciones de datos deben tener propósitos y funciones definidos.

F.10. Existen controles adecuados sobre los equipos de prueba de comunicaciones usados para monitoreas líneas y fijar problemas incluyendo:

- Procedimiento restringido el uso de estos equipos a personal autorizado.
- Facilidades de traza y registro del tráfico de datos que posean los equipos de monitorización.
- Procedimientos de aprobación y registro ante las conexiones a líneas de comunicaciones en la detección y corrección de problemas.

F.11. En el plan general de recuperación de desastres para servicios de información presa adecuada atención a la recuperación y vuelta al servicio de los sistemas de comunicación de datos.

F.12. Existen planes de contingencia para desastres que sólo afecten a las comunicaciones, como el fallo de una sala completa de comunicaciones.

F.13. Las alternativas de respaldo de comunicaciones, bien sea con las mismas salas o con salas de respaldo, consideran la seguridad física de estos lugares.

F.14. Las líneas telefónicas usadas cuyos números no deben ser públicos, tiene dispositivos/procedimientos de seguridad tales como retro llamada, códigos de conexión o interruptores para impedir accesos no autorizados al sistema informático.

6.1.2. Planeación de Auditoria de Red Lógica

Es necesario monitorizar la red, los errores o situaciones anómalas que se producen y tener establecidos los procedimientos para detectar y aislar equipos en situación anónima. En general, se quiere que la información que viaja por la red no pueda ser espiada o alterada, la única solución totalmente efectiva es la encriptación.

En la planeación de la auditoría lógica de la red, Como objetivos de control, se deben marcar la existencia de:

- Contraseñas y otros procedimientos para limitar y detectar cualquier intento de acceso no autorizado aka red de comunicaciones.
- Facilidades de control de errores para detectar errores de trasmisión y establecer las retransmisiones apropiadas.
- Controles para asegurar que las transmisiones van solamente a usuarios autorizados y que los mensajes no tienen por qué seguir siempre la misma ruta.
- Registro de la actividad de la red, para ayudar a reconstruir incidentes y detectar accesos no autorizados.
- Técnicas de cifrado de datos donde haya riesgos de accesos impropios a trasmisiones sensibles.
- Controles adecuados que cubran la importación o exportación de datos a través de puertas, en cualquier punto de la red, a otros sistemas informáticos.

6.1.2.1. Ejecución de Auditoria de Red Lógica

Listas de control

Comprobar que:

L.1. El software de comunicaciones, para permitir el acceso, exige código de usuario y contraseña.

L.2. Revisar el procedimiento de conexión de usuario y comprobar que:

- Los usuarios no pueden acceder a ningún sistema, no siquiera de ayuda, antes de haberse identificado correctamente.
- Se inhabilita al usuario que sea incapaz de dar la contraseña después de un número determinado de intentos infructuosos.
- Se obliga a cambiar la contraseña regularmente.

- Las contraseñas no son mostradas en pantalla cuando se teclean.
- Durante el procedimiento de identificación, los usuarios son informados de cuándo fu su última conexión para ayudar a identificar potenciales suplantaciones o accesos no autorizados.

L.3 Cualquier procedimiento del fabricante, mediante hardware o software, que permita el libre acceso y que haya sido utilizado en la instalación original, ha de haber sido inhabilitado o cambiado.

L.5. Los protocolos utilizados, revisados con el personal adecuado de comunicaciones, disponen de procedimientos de control de errores con la seguridad suficiente.

L.4. Se toman estadísticas que incluyan tasas de errores y de retransmisión.

L.6. Los mensajes lógicos transmitidos identifican el origen, la fecha, la hora y el receptor.

L.7. El software de comunicaciones ejecuta procedimientos de control y correctivos ante mensajes duplicados, fuera de orden, perdido o retrasados.

L.8. La arquitectura de comunicaciones utiliza indistintamente cualquier ruta disponible de transmisión para minimizar el impacto de una escucha de datos sensibles en una ruta determinada.

L.9. Existen controles para que los datos sensibles sólo puedan ser impresos en las impresoras designadas y vistos desde terminales autorizados.

L.10. Existen procedimientos de registro para capturar y ayudar a reconstruir todas las actividades de las transacciones.

L.11. Los archivos de registro son revisados, si es posible a través de herramientas automáticas, diariamente, vigilando intentos impropios de acceso.

L.12. Existen análisis de riesgos para las aplicaciones de proceso de datos a fin de identificar aquellas en las que el cifrado resulte apropiado.

L.13. Si se utiliza cifrado:

- Existen procedimientos de control sobre la generación e intercambio de claves.
- Las claves de cifrado son cambiadas regularmente.
- El transporte de las claves de cifrado desde donde se generan a los equipos que las utilizan siguen un procedimiento adecuado.

L.14. Si se utilizan canales de comunicación uniendo diversos edificios de la misma organización y existen datos sensibles que circules por ellos, comprobar que estos

canales se cifran automáticamente, para evitar que una intercepción sistemática a un canal comprometa a todas las aplicaciones.

L.15. Sila organización tiene canales de comunicación con otras organizaciones se analice la conveniencia de cifrar estos canales.

L.16. Si se utiliza la transmisión de datos sensibles a través de redes abiertas como internet, comprobar que estos datos viajan cifrados.

L.17. Si una red local existe computadoras con módems, se han revisado los controles de seguridad asociados a para impedir el acceso de equipos foráneos a la red local.

L.18. Existe una política de prohibición de introducir programas personales o conectar equipos privados a la red local.

L.19. Todas las "puertas traseras" y accesos no específicamente autorizados están bloqueadas. En equipos activos de comunicaciones, como puentes, encaminadores, conmutadores, etc., esto significa que los accesos para servicio remoto están inhabilitados o tiene procedimientos específicos de control.

L.20. Periódicamente se ejecutan, mediante los programas actualizados y adecuados, ataques para descubrir vulnerabilidades, que los resultados se documentan y se corrigen las deficiencias observadas.

6.1.3. Planeación de Auditoría de Web

Una auditoría web consiste en el análisis y posterior corrección de los errores detectados en una página web o un blog, así como la implantación de las mejoras necesarias con el fin de lograr optimizar sus distintos elementos, tanto de diseño como de contenidos, estructura etc.

De esta forma, se logra un mejor posicionamiento, mayor tráfico y más conversiones y, por lo tanto, un aumento de la rentabilidad.

Para que sea útil y fiable, una auditoría web debe analizar tres aspectos básicos de nuestra página o blog:

1. **Usabilidad:** La usabilidad es la facilidad y comodidad con la que los usuarios navegan por nuestra web. En este aspecto, una auditoria nos puede resultar de inestimable ayuda para detectar: enlaces rotos, ralentizaciones excesivas de la

velocidad de carga de la página o de algunas de sus partes (sobre todo a través de teléfonos móviles), menús poco claros u otros problemas de navegación.

En conjunto, la subsanación de estos errores puede mejorar enormemente la usabilidad del usuario, mejorando también su experiencia y consiguiendo que las visitas que entren en nuestra página repitan y se queden más tiempo con nosotros.

2. **Optimización:** Un segundo aspecto fundamental en una auditoria web es analizar todos aquellos aspectos (que son muchos y variables) que influyen en el algoritmo de Google y que, por lo tanto, van a acabar determinando nuestra posición en la SERP tras las búsquedas de los usuarios:
    - Estructura de las URL.
    - Calidad de los contenidos.
    - Estrategia de palabras clave o keywords.
    - Arquitectura del sitio.
    - Número y calidad de los enlaces internos y externos.
    - Planificación de la presencia de la web en redes sociales y plataformas profesionales.
3. **Seguridad:** Uno de los aspectos cada vez más valorados y exigidos por los usuarios de una página web es la seguridad, especialmente cuando entran en juego datos personales o de especial sensibilidad, como los relacionados con la salud o los bancarios.

    De ahí la necesidad de detectar a tiempo cualquier tipo de vulnerabilidad o debilidad que permite que un tercero pueda hacer un uso fraudulento de dichos datos.

De esta forma, conoceremos con objetividad y exactitud cuál es el estado de salud de nuestra página, disponiendo de una información fundamental para: mejorar el posicionamiento en las entradas de Google y otros buscadores, conseguir más tráfico, aumentar el porcentaje de conversión de visitas a registros (leads) y a clientes reales, o ganar en prestigio y autoridad, entre otras ventajas.

Los objetivos de una Auditoria Web son:

- Detectar puntos débiles para corregirlos.
- Potenciar los puntos fuertes.

- Analizar la usabilidad y navegabilidad optima de la web.
- Optimizar el sitio para poder ser indexado correctamente por los buscadores.

6.1.3.1. Ejecución de Auditoria de Web

En la ejecución de la auditoría se aplican las herramientas, métodos y técnicas de trabajo necesarias para cumplir con los objetivos planeados.

Mediante la técnica del cuestionario o entrevista se procede a revisar los siguientes detalles de la web:

Información general e identificación:

- Nombre de la organización.
- Logotipo.
- Slogan publicitario.
- Datos sobre los productos y servicios que se ofertan.
- Informaciones de contacto de la entidad: Nombre del gerente, Dirección postal y virtual, teléfonos, fax, e-mail, etc.
- Informaciones sobre la actividad de la entidad.
- Información sobre sucursales de la entidad.

Precisión, confiabilidad y exactitud:

- Calidad de la digitalización y tipografía.
- Referencia a las fuentes informativas utilizadas, con objetivos de comprobación o ampliación.
- Información sobre los autores de los contenidos, y contactos (directo, indirecto) con los mismos. Resumen de su curriculum vitae.
- Fechas de creación y de actualización del sitio, así como de los materiales utilizados.
- Seguridad de los hipervínculos.
- Datos de los Proveedores de Servicios de Certificación y Autentificación (sí existe): nombre, e-mail, dirección postal y virtual, teléfono, fax, etc.

Amplitud informativa:

- Alcance de los temas tratados.
- Actualidad de estos temas.

- Citas debidamente cumplimentadas.
- Relación entre la misión, objetivos y funciones de la organización y los contenidos informativos presentados.
- Prestigio de los autores de los materiales presentados.
- Aptitud de la entidad y los autores para tratar los temas presentados.
- Vínculos a los sitios que presentan ampliación de la información de los temas.

Aptitud:

- Información sobre capacidad de la organización para abordar los temas presentados.
- Conocimiento de la organización.
- Relación de los autores de los temas con el contenido de los mismos.
- Opiniones de otras organizaciones o personalidades sobre los temas expuestos.

Capacidad comunicativa:

- Revisar estadísticas de visita del sitio.
- Aplicación de los anuncios publicitarios.
- Balance de información textual, gráfica e imágenes.
- Lenguaje preciso y adecuado a los posibles receptores.
- Idiomas utilizados.

Contenido básico:

- Relación entre las informaciones del sitio y el propósito fundamental de la organización.
- Profundidad, confiabilidad y validez de los temas tratados.
- Autoridad profesional de los autores y la organización con relación a los aspectos tratados

Sintáctica:

- Calidad en la ortografía, la redacción, la puntuación, los gráficos, las imágenes, los sonidos.
- Calidad en los textos completos, en los de resumen y de la información factográfica.

Promoción y divulgación:

- Calidad de los banners, los mensajes publicitarios, los logotipos de los anunciantes, sus datos, etc.
- Promociones publicitarias.

Diseño y arquitectura:

- Calidad de la atracción del diseño.
- Variedad y calidad de las imágenes.
- Facilidad de acceso a las imágenes.
- Combinación ergonómica adecuada de los colores del fondo, las letras y los gráficos.
- Calidad estética de los gráficos, las imágenes, los textos y el resto de los diseños.
- Arquitectura adecuada del sitio.

Accesibilidad:

- Menús fáciles de acceder, en todos los niveles del sitio.
- Retornos fáciles.
- Historia de acceso, para facilitar la reproducción del mismo.
- Opciones de inscripción sencillas.
- Opciones de pago por utilización de la información.
- Empleo de software general.
- Descarga sencilla de información o aplicaciones.
- Utilización de motores de búsqueda adecuados y difundidos.
- Opciones de búsqueda diferentes.
- Rutina de trabajo eficiente.

Utilidad:

- Estadísticas de accesos al sitio.
- Estadísticas de información bajada del sitio.
- Acciones generadas por las consultas del sitio (negocios, consultas, etc.)
- Económicos y financieros.
- Costo del acceso.

Económicos y financieros:

- Costo del acceso.
- Fuerza de trabajo empleada en la confección y actualización del sitio.
- Costo de los servicios de conectividad.
- Costo de la adquisición y amortización de los activos fijos intangibles (software, licencias, patentes, etc.)
- Costo de la adquisición y amortización de activos fijos tangibles.
- Utilidad generada por el sitio.
- Rentabilidad del sitio.

Profesional:

- Misión y objetivos del sitio.
- Ética de la entidad.
- Declaraciones de la responsabilidad del sitio.
- Información sobre las actividades de la organización.

Valor añadido:

- Servicios en línea que presta.
- Formularios para interactuar con la organización.
- Noticias actualizadas sobre temáticas de interés para los clientes.
- Información sobre mecanismos de consulta, baja de información, venta, etc.
- Información sobre servicios de postventa.
- Facilidades de pago. Ventajas. Estímulos. Promociones.
- Entretenimientos.
- Buzones de quejas y sugerencias.
- Servicios adicionales: asesoría, etc.
- Interacción con otros recursos de Internet.

Desempeño:

- Rapidez de consulta.
- Velocidad al bajar las imágenes.

EJERCICIO PRÁCTICO 1:

1. Investiga que medidas de seguridad lógica en la red hay implantadas en uno de los laboratorios de informática de la Universidad Tecnológica de Panamá y explica cómo se podrían mejorar.

EJERCICIO PRÁCTICO 2:

1. Realice una auditoría de la seguridad de la red de la Compañía W, basándose en la siguiente información:

La compañía W es una empresa de software. Su modelo de negocio se basa en transacciones electrónicas con proveedores y clientes clave. La compañía W usa una implementación de BizTalk Server para sus transacciones.

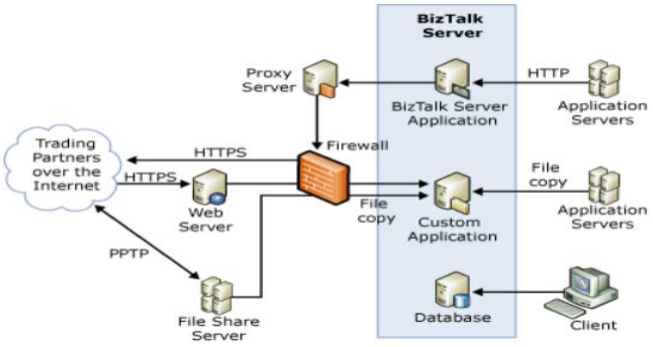
Usa BizTalk Server para administrar transacciones y las comunicaciones entre aplicaciones internas y externas. Se comunica con 85 aplicaciones internas y 2300 socios comerciales (aproximadamente). Actualmente procesa aproximadamente 2,5 millones de documentos al mes, pero estima que a finales de 2007 llegará a procesar 6 millones de documentos mensualmente.

Aspectos relacionados con la seguridad y posibles amenazas

La compañía W quiere asegurarse de que sólo va a recibir y procesar mensajes cuyo origen esté autenticado. La compañía W también desea asegurarse de que puede recibir y recuperar documentos procedentes del exterior de su red corporativa de la forma más segura posible. El servidor de seguridad que separa la red corporativa de la compañía W de Internet sólo deja pasar tráfico de los puertos 80 y 443. El firewall rechaza todo el tráfico restante.

Arquitectura de seguridad

En la ilustración siguiente, se muestra la arquitectura que utiliza la compañía W.



La compañía W utiliza BizTalk Server como agente de mensajes para la comunicación entre las aplicaciones internas y para procesar y enviar mensajes con el formato correcto a sus proveedores y clientes, y recibir mensajes de éstos. La compañía W tiene que procesar documentos internos y externos con diferentes formatos, incluidos los archivos sin formato y los documentos XML.

La compañía W utiliza un único servidor de seguridad para separar sus equipos corporativos de Internet. Como nivel de seguridad adicional, la compañía W incorpora la seguridad del protocolo de Internet (IPsec) para la comunicación entre todos los servidores y estaciones de trabajo que se encuentran dentro de la red corporativa. La compañía W utiliza IPsec para cifrar todas las comunicaciones dentro de su dominio interno.

La compañía W utiliza un servidor de recursos compartidos de archivos para recibir archivos sin formato. Este servidor de recursos compartidos se encuentra fuera del dominio y la red de la empresa. Un servidor de seguridad separa el servidor de recursos compartidos de archivos de la red corporativa. Los socios externos de la compañía W publican sus documentos como archivos sin formato en el servidor de recursos compartidos de archivos y se comunican con éste a través de un Protocolo de túnel punto a punto (PPTP). La compañía W protege el acceso al servidor de recursos compartidos de archivos mediante contraseñas de socio que caducan cada 30 días.

La compañía W ha creado una aplicación personalizada para el traslado de archivos que recupera los documentos sin formato del servidor de recursos compartidos de archivos y los envía a BizTalk Server para someterlos a un procesamiento adicional.

Las aplicaciones internas de la compañía W también utilizan esta aplicación personalizada para pasar archivos sin formato a BizTalk Server. BizTalk Server transforma estos documentos y los envía a los socios comerciales de la compañía W.

Antes de transformar los datos del socio en formatos de aplicación internos, BizTalk Server comprueba si disponen de entradas para el remitente, el receptor y el tipo de documento. Si BizTalk Server recibe un mensaje que no tiene entradas de remitente, receptor o tipo de documento, lo rechazará. El equipo de operaciones de la compañía W se encargará de analizar el mensaje. Las aplicaciones internas envían mensajes en diversos formatos (EDIFACT, archivo sin formato, XML y ANSI X12).

La compañía W también recibe documentos de origen interno y externo a través de HTTPS. Los asociados externos publican sus documentos en un servidor Web que se encuentra fuera de la red corporativa. Un servidor de seguridad separa este servidor Web de la red corporativa. La aplicación personalizada para el traslado de archivos también recupera los documentos publicados a través de HTTPS. La compañía W utiliza un producto de terceros para cifrar y firmar los mensajes dirigidos a sus socios comerciales. Como medida de seguridad adicional, se realiza una auditoría nocturna en todos los servidores para asegurarse de que la configuración de seguridad es correcta. Se registran todas las excepciones para revisarlas.

EJERCICIO PRÁCTICO 3

Basado en la auditoría web responda las siguientes preguntas:

1. Explica para qué sirve el sello de Confianza online en cuanto a seguridad se refiere.

2.- ¿Para qué sirve google Analytics? ¿Cuál es el uso que hace google analytics de nuestros datos? Explica con detalle y entendiendo lo que escribes, cómo lo hace Google Analytics para revisar las estadísticas.

BIBLIOGRAFÍA:

- Lázaro Blanco. (2001). Auditoría a Sitios Web. Universidad de la Habana. Artículo Digital.
- Carrasco Luis. (2012). Redes de Anonimización en Internet. Ieee.es (Instituto Español de Estudios Estratégicos). Artículo de opinión.
- Giménez Francisco. (2014). Seguridad en equipos informáticos. IFCT0109. IC Editorial. España.
- Areitio Javier. (2010) “Test de seguridad para evaluar y mejorar el nivel de riesgos de seguridad”.
- Areitio, J. “Seguridad de la Información: Redes, Informática y Sistemas de Información”. Cengage Learning-Paraninfo. 2009.
- Piattini, Mario G. del Peso, Emilio. (2001) Auditoría Informática un Enfoque Práctico. Editorial Computec.
- PINILLA, José D. Auditoría Informática un Enfoque operacional. Editorial Ecoe.